National Risk Estimate:
Risks to U.S. Critical Infrastructure from Insider Threat

National Protection and Programs Directorate
Office of Infrastructure Protection
Integrated Analysis Task Force
Homeland Infrastructure Threat and Risk Analysis Center

Homeland Security

December 2013

This page intentionally left blank.

Executive Summary

The Department of Homeland Security's (DHS) Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) produced this National Risk Estimate (NRE) to provide an authoritative, coordinated, risk-informed assessment of the key security issues faced by the Nation's infrastructure protection community from malicious insiders. DHS used subject matter expert elicitations and tabletop exercises to project the effect of historic trends on risks over the next 3 to 5 years. In addition, DHS used alternative futures analysis to examine possible futures involving insider threats to critical infrastructure over the next 20 years. The results are intended to provide owners and operators a better understanding of the scope of the threat and can inform mitigation plans, policies, and programs, particularly those focused on high-impact attacks.

The malicious insider threat is complex and dynamic, and it affects the public and private domains of all 16 critical infrastructure sectors. Owners and operators responsible for protecting our nationally-critical assets must recognize the nuances and breadth of this threat in order to develop appropriate risk-based mitigation strategies.

Current Risk Assessment

Understanding and mitigating insider threat are complicated by factors such as technological advances, globalization, and outsourcing. These factors increasingly blur the line between traditional insiders and external adversaries such as terrorists, organized crime groups, and foreign nation-states, who may collude with or exploit physical insiders as vectors to do harm to a targeted asset or system. The threat of supply chain sabotage by third-party vendors and contractors was a recurring theme that subject matter experts discussed during the NRE workshops and tabletop exercises. All agreed that the third-party insiders constitute an underestimated threat to U.S. critical infrastructure, particularly when their organizations are foreign-owned or are working under the auspices of foreign intelligence services.

The common feature of all malicious insiders is tactical advantage. Sometimes the insiders are organizational vulnerabilities—adversarial force multipliers—who can operate relatively unfettered. Malicious insiders are not only aware of an organization's vulnerabilities; they also may have purposefully created the very vulnerabilities they intend to exploit.

Although the importance of understanding and mitigating the insider threat is clear, two major factors complicate current efforts to assess the likelihood of malicious insider attacks:

- The challenge of identifying and predicting the stressors or triggers that can cause a trusted employee to become a malicious actor; and
- The lack of detailed and reliable empirical data on insider breaches and attacks that can be shared across the full spectrum of critical infrastructure owners and operators.

The available data do not characterize in detail the full scope of insider threat to U.S. critical infrastructure and do little to explain why the United States has not experienced a significant increase in insider attacks, particularly those that could result in high-to-catastrophic consequences. They do, however, provide a starting point from which to create a baseline threat profile that can be used to assess insider threats across the 16 critical infrastructure sectors.

KEY FINDINGS AND RECOMMENDATIONS

The Threat: Malicious Insiders

- Access and specialized knowledge give insiders tactical advantages over security efforts.
- Technological advances, globalization, and outsourcing increasingly blur the line between traditional insiders and external adversaries.
- Insiders who combine advanced technological understanding with traditional espionage/terrorist skills have a significantly increased asymmetric capability to cause physical damage through cyber means.

The Vulnerabilities: Expanding Organizational Security Boundaries

- Even sectors with relatively robust preventative programs and guidelines in place face a dynamic and expanding threat that cannot be eliminated altogether.
- Some organizations are likely underestimating the threat from third-party insiders such as vendors and contractors.
- Industrial control systems in critical infrastructure are attractive insider targets for remote sabotage in an increasingly networked world.
- Without credible and sector-specific insider risk information, critical infrastructure owners and operators are likely to underestimate the scope of the malicious insider threat and make insufficient or misdirected investments in security.

The Consequences: Asymmetric Impacts

- If the goal of malicious insider activity is exploitation rather than destruction of assets, it will be more difficult to detect, potentially resulting in serious cumulative consequences.
- The impacts of a cyberattack that is designed to cause physical damage to critical infrastructure could be much more severe than those of a conventional cyberattack.

Recommendations

- The Government and private sector should work to develop comprehensive and scalable insider threat program standards that incorporate long-term employee monitoring policies, including background checks and re-investigations, employee training and termination of access at separation.
- Effective prevention and mitigation programs must be driven by better understanding the insider's definition of success against a particular sector.
- Organizations should establish workforce behavioral and access baselines, including an understanding of hiring, oversight, access, and security policies, in order to identify anomalies.
- Employees used as a monitoring force may be the best way to identify malicious insiders, and they must have access to recurring training to do so effectively.
- Public and private organizations must consider how to balance the best risk-based security procedures against the myriad of policy, legal, and employees' rights issues associated with obtaining and analyzing relevant threat data in the workplace, especially data derived from social media and behavioral monitoring.

Exploring Alternative Futures

In addition to the work done with this NRE, DHS also hosted a one-day workshop specifically to elicit subject matter expert judgment on four alternative futures that could present challenges and opportunities related to malicious insider threats to U.S. critical infrastructure over the next 20 years. The alternative futures are not intended to predict the future but to examine plausible combinations of uncertainties and contributing factors that tell a series of compelling stories about the nature and mitigation of the insider threat.
Participants selected two major uncertainties, **governance** and **insider capabilities**, as the drivers for the alternative futures related to insider risk to the 16 U.S critical infrastructure sectors.

Two of the resulting scenarios, designated Advantage Good Guys (Traditional Insider Capabilities—Effective Governance) and Mission Impossible (Technologically-Enhanced Insider Capabilities—Haphazard Governance), present the most compelling challenges for U.S. critical infrastructure stakeholders in the combination of uncertainties and variables highlighted.

- In the Advantage Good Guys future, the traditional insider must work hard and risk exposure to identify and target what is *not* guarded in his or her domain to be successful. Effective governance creates a higher probability of detection, greatly reducing the overall risk of an insider attack. In this world, insider collusion may become an imperative to overcome layered defenses with more physical and cyber threat mitigation controls in place.
- In the Mission Impossible scenario, the insider is more capable with enhanced tradecraft than ever before, making effective risk management more difficult, if not impossible. A non-standardized culture of governance sets the scene for repeatable and systemic attacks by insiders using technologically enhanced techniques to launch targeted and potentially widespread attacks from one or multiple vectors with minimal risk of attribution. Insiders who have worked their way up the company chain may have played a role in building the haphazard governance and infrastructure they seek to exploit. Outsourcing continually broadens the field of potential adversaries in the U.S. critical infrastructure virtual supply chain. The "high-tech" insiders have a significantly enhanced asymmetric capability to create widespread kinetic impact though cyber means. Perhaps more highly destructive is their ability to conduct widespread cyber exploitation attacks, the effects of which cannot be seen before potentially catastrophic consequences result.

Key trends that will affect the future insider threat landscape over the next 20 years include the continued viability of traditional, "low-tech" insider techniques to exploit gaps in the prevailing security environment, migration to and dependence upon the "cloud," increased potential for blended (cyber and physical) attacks, globalization, and outsourcing. These latter trends increasingly will force owners and operators to collaborate and exchange data via external/third party IT networks over whose security they have little to no control.

Risk Mitigation

Existing best practices should inform mitigation measures, but the nature of the insider threat leads to specific areas that are particularly challenging, and in which there are opportunities to strengthen current measures against malicious insiders. During the tabletop exercises and the

Alternative Futures workshop in support of the NRE, subject matter experts identified the following issues as particularly challenging for insider risk mitigation:

- Acknowledging and dealing with a pervasive threat;
- Breaching roadblocks to public-private cooperation and information sharing;
- Establishing workforce behavioral and access baselines;
- Implementing effective employee insider threat training programs;
- Incorporating public information campaigns into response and recovery;
- Refining incident response to contain technically adept insiders; and
- Understanding the psychology of a malicious insider.

Table of Contents

Chapter 1: Purpose and Scope

Purpose

The Department of Homeland Security's (DHS) Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) produced this National Risk Estimate (NRE) to provide an authoritative, coordinated, risk-informed assessment of the key security issues faced by the Nation's infrastructure protection community from malicious insiders. DHS used subject matter expert elicitations and tabletop exercises to project the effect of historic trends on risks over the next 3 to 5 years. In addition, DHS used alternative futures analysis to examine possible futures involving insider threats to critical infrastructure over the next 20 years. The results are intended to provide owners and operators a better understanding of the scope of the threat and can inform mitigation plans, policies, and programs, particularly those focused on high-impact attacks.

The Need to Assess Insider Threat Risks

The following key documents address the U.S. Government concerns about insider threat and the need to assess associated risks:

- DHS *2011 National Risk Profile (NRP)*, November 2011. Through the NRP process, stakeholders and partners identified insider threat as an area of concern for DHS to address.[1]
- Executive Order (EO) 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, signed by the President on October 7, 2011. The EO establishes an insider threat task force to develop a Government-wide insider threat program for deterring, detecting, and mitigating insider threats.[2]
- DHS *National Infrastructure Protection Plan (NIPP)*, 2009. Under the NIPP's well-established policy guidance, guarding against insider threat is a U.S. critical infrastructure owner and operator risk management function.[3]
- National Infrastructure Advisory Council (NIAC) report, *The Insider Threat to U.S. Critical Infrastructures, 2008*. The NIAC report identified insider threat as an area requiring research to improve programs and resource allocation by critical infrastructure owners and operators.[4]

[1] National Protection and Programs Directorate/Office of Infrastructure Protection, *Appendix B: 2011 National Risk Profile*, Washington, D.C.: U.S. Department of Homeland Security, November 2011: B-v.
[2] Executive Order 13578, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 2011: 4.
[3] Office of Infrastructure Protection, *National Infrastructure Protection Plan*, Washington, D.C.: U.S. Department of Homeland Security, 2009: 24-25
[4] Noonan, Thomas and Edmund Archuleta, *The National Infrastructure Advisory Council's Final Report and Recommendations on The Insider Threat to Critical Infrastructure*, Washington, D.C.: National Infrastructure Advisory Council, 2008: 38.

Scope

This NRE considers historic trends in insider threats as they affect risks over the next 3 to 5 years, alternative futures pertaining to insider threat to critical infrastructure over the next 20 years, and measures to mitigate insider threat to U.S. critical infrastructure.

Analysis focuses on insiders with varying levels of access to systems, facilities, or information. Also considered are others with access and inside knowledge, such as former employees and third-party or trusted business partners, e.g., contractors, sub-contractors, consultants, temps, students, and service/IT vendors who support a critical infrastructure. Hackers (individuals or groups) are excluded, however, since they operate almost exclusively from outside a given target.

The NRE uses the definition of insider threat developed by the NIAC in a 2008 study:

> "*The **insider threat** to critical infrastructure is one or more individuals with the access and/or insider knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with intent to cause harm*."[5]

The literature review conducted in support of this NRE highlighted three recurring insider threat themes:

- **Terrorism**, which involves premeditated, politically motivated violence perpetrated against noncombatant targets by groups or clandestine agents.[6]
- **Espionage**, which is the practice of spying or using spies to obtain secret or sensitive technology or information about the plans and activities of another organization, including a foreign government or a competing company.[7]
- **Corruption**, which is securing an advantage through means which are inconsistent with one's duty or the rights of others.[8]

The NRE's scenario-based risk assessment uses insider scenarios that were developed across the 16 U.S. critical infrastructure sectors, as well as the themes of terrorism, espionage, and corruption.(these scenarios are summarized in Table 1 on pages 17 to 20 of this report).

Data supporting the work was drawn from unclassified government, academic, and private sector reporting and analysis as well as from the judgments of subject matter experts.

The analysis addresses the following overarching questions:

---

[5] Noonan, Thomas and Edmund Archuleta, *The National Infrastructure Advisory Council's Final Report and Recommendations on The Insider Threat to Critical Infrastructure*, Washington, D.C.: National Infrastructure Advisory Council, 2008: 11.

[6] Definition contained in Title 22 of the U.S. Code, Section 2656f(d) and used by the Intelligence Community.

[7] Adapted from Gelles, Michael, David Brant, and Brain Geffert, *Building a Secure Workforce*. Deloitte Consulting LLP, 2008: 2, www.deloitte.com/view/en_US/us/Industries/US-federal-government/764ef33b4010e110VgnVCM100000ba42f00aRCRD.htm, accessed April 25, 2012.

[8] Gelles, Michael and John Cassidy, *Security Along the Border: The Insider Threat*, Deloitte Consulting, LLP, 2011: 8, www.deloitte.com/view/en_US/us/Industries/US-federal-government/federal-focus/homeland-security/a889e5fa3349d210VgnVCM3000001c56f00aRCRD.htm, accessed April 25, 2012.

- Are there notable trends with respect to the risk of insider threat posed to U.S. critical infrastructure?
- How will the insider threat to critical infrastructure sectors likely evolve over the next 20 years?
- What is the current capability (both domestic and international) to mitigate insider threats that affect U.S. critical infrastructure?

The following underlying analytic assumptions, developed by eliciting input from various expert participants, guide the analysis for this NRE:

- Insider threats to U.S. critical infrastructure will continue;
- Malicious insiders will be more technologically savvy and increasingly capable of defeating security countermeasures that are static, improperly scoped, or unable to keep pace with the evolving threat;
- The line between internal and external threats will be increasingly blurred because of the proliferation of digital, Web-based technology within business and control systems;
- Major investments in U.S. critical infrastructure to mitigate insider threats will not be universal or consistent; and
- Innovation and effective risk management will be able to mitigate certain aspects of insider threat risk.

Summary of the NRE Development Approach

The findings contained in this NRE are informed by a comprehensive literature review and by input elicited from Federal Government and private sector subject matter experts. Moreover, a formal analytic process supports the risk analysis across the 16 U.S. critical infrastructure sectors. The limited availability of insider threat data means that there is uncertainty associated with the NRE risk assessments.

The NRE development process consists of three phases: research and planning, workshops and exercises, and analysis and coordination.

- The **research and planning phase** included a literature review, development of the Terms of Reference document, consultation with subject matter experts about development of insider threat scenarios, and planning for the NRE workshops and tabletop exercises, including contacting and arranging for the participation of appropriate subject matter experts.
- The **workshops and exercises phase** included an alternative futures workshop and three tabletop exercises addressing various aspects of insider threat and U.S. critical infrastructure.

  The Alternative Futures workshop developed information for the outlook section of the NRE. The methodology for this was based on the methodology used by the Office of the Director of National Intelligence's National Intelligence Council (NIC) in their *Global Trends 2025* National Intelligence Estimate and described in a 2008 NIC report on

disruptive civil technologies.[9] This approach also was used to develop the information for outlook sections of the two previous DHS NREs (1) *Risks to U.S. Critical Infrastructure from Supply Chain Disruptions* in 2010 and (2) *Risks to U.S. Critical Infrastructure from GPS Disruptions* in 2011.

The three one-day tabletop exercises addressed the three insider threat themes considered in this NRE--terrorism, espionage, and corruption. Each exercise involved a Red Team exploiting vulnerabilities and developing several attack plans and a Blue Team developing a response to each plan to prevent, protect from, mitigate, respond to, and recover from the attack. The exercises provided insights into adversary planning and decisionmaking.

- The **analysis and coordination phase** involved the drafting of the NRE, with an interagency effort to review the NRE for soundness, consistency, and accuracy. This phase included an assessment of the risks to critical infrastructure from insider threat and helps identify key insider threat trends gleaned from the research and the results of the workshop and exercises. During this phase, the analysis also identified potential strategies for the public and private sectors that could mitigate the insider threat to U.S. critical infrastructure.

The NRE has been coordinated with DHS components, the Intelligence Community, other Federal agencies, national laboratories, private sector partners, and academia.

[9] U.S. National Intelligence Council, *Disruptive Civil Technologies: Six Technologies with Potential Impacts on U.S. Interests Out to 2025*, Conference Report CR 2008-07, April 2008, www.fas.org/irp/nic/disruptive.pdf, accessed March 15, 2012.

Chapter 2: Key Findings and Recommendations

The malicious insider threat is complex, dynamic, and affects the public and private domains of all 16 critical infrastructure sectors. Owners and operators responsible for protecting our nationally critical assets must recognize the nuances and breadth of this threat in order to develop appropriate risk-based mitigation strategies. All owners and operators of critical infrastructure, whether publically traded, privately held, or public sector, are responsible to their stakeholders for making sufficient and cost-effective investments in security. Without clear-cut, sector-specific, and credible threat information, owners and operators are likely to underestimate the threat and may under-invest in security or misdirect resources.

For this analysis, DHS adopted the definition of insider threat developed by the National Infrastructure Advisory Council (NIAC) in its 2008 study:

> "The **insider threat** to critical infrastructure is one or more individuals with the access and/or insider knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with intent to cause harm."[10]

Based on this definition, the analysis includes former employees and third-party or trusted business partners, such as contractors, consultants, temporary hires, students, and service/information technology (IT) vendors supporting critical infrastructure, who have inside access to an organization, but does not consider outside hackers.

[10] Noonan, Thomas and Edmund Archuleta, *The National Infrastructure Advisory Council's Final Report and Recommendations on The Insider Threat to Critical Infrastructure*, Washington, D.C.: National Infrastructure Advisory Council, 2008: 11.

KEY FINDINGS AND RECOMMENDATIONS

The Threat: Malicious Insiders

- Access and specialized knowledge give insiders tactical advantages over security efforts.
- Technological advances, globalization, and outsourcing increasingly blur the line between traditional insiders and external adversaries.
- Insiders who combine advanced technological understanding with traditional espionage/terrorist skills have a significantly increased asymmetric capability to cause physical damage through cyber means.

The Vulnerabilities: Expanding Organizational Security Boundaries

- Even sectors with relatively robust preventative programs and guidelines in place face a dynamic and expanding threat that cannot be eliminated altogether.
- Some organizations are likely underestimating the threat from third-party insiders such as vendors and contractors.
- Industrial control systems in critical infrastructure are attractive insider targets for remote sabotage in an increasingly networked world.
- Without credible and sector-specific insider risk information, critical infrastructure owners and operators are likely to underestimate the scope of the malicious insider threat and make insufficient or misdirected investments in security.

The Consequences: Asymmetric Impacts

- If the goal of malicious insider activity is exploitation rather than destruction of assets, it will be more difficult to detect, potentially resulting in serious cumulative consequences.
- The impacts of a cyberattack that is designed to cause physical damage to critical infrastructure could be much more severe than those of a conventional cyberattack.

Recommendations

- The Government and private sector should work to develop comprehensive and scalable insider threat program standards that incorporate long-term employee monitoring policies, including background checks and re-investigations, employee training and termination of access at separation.
- Effective prevention and mitigation programs must be driven by better understanding the insider's definition of success against a particular sector.
- Organizations should establish workforce behavioral and access baselines, including an understanding of hiring, oversight, access, and security policies, in order to identify anomalies.
- Employees used as a monitoring force may be the best way to identify malicious insiders, and they must have access to recurring training to do so effectively.
- Public and private organizations must consider how to balance the best risk-based security procedures against the myriad of policy, legal, and employees' rights issues associated with obtaining and analyzing relevant threat data in the workplace, especially data derived from social media and behavioral monitoring.

Current Risk Assessment

Understanding and mitigating insider threat are complicated by factors such as technological advances, globalization, and outsourcing. These factors increasingly blur the line between traditional insiders and external adversaries such as terrorists, organized crime groups, and foreign nation-states, who may collude with or exploit physical insiders as vectors to do harm to a targeted asset or system. The threat of supply chain sabotage by third-party vendors and contractors was a recurring theme that subject matter experts discussed during the NRE workshops and tabletop exercises. All agreed that the third-party insiders constitute an underestimated threat to U.S. critical infrastructure, particularly when their organizations are foreign-owned, raising possibility of ties to foreign government interests.

The common feature of all malicious insiders is tactical advantage. In essence, the insiders are organizational vulnerabilities—adversarial force multipliers—who can operate relatively unfettered. Not only do malicious insiders know an organization's vulnerabilities, they can intentionally create vulnerabilities that they intend to exploit.

Although the importance of understanding and mitigating the insider threat is clear, two major factors complicate current efforts to assess the likelihood of malicious insider attacks:

- The challenge of identifying and predicting the stressors or triggers that can cause a trusted employee to become a malicious actor; and
- The lack of detailed and reliable empirical data on insider breaches and attacks that can be shared across the full spectrum of critical infrastructure owners and operators.

The available data do not characterize in detail the full scope of insider threat to U.S. critical infrastructure and do little to explain why the United States has not experienced a significant increase in insider attacks, particularly those that could result in high-to-catastrophic consequences. They do, however, provide a starting point from which to create a baseline threat profile that can be used to assess insider threats across the 16 critical infrastructure sectors.

Exploring Alternative Futures

DHS hosted a one-day workshop to elicit subject matter expert judgment on four alternative futures that could present challenges and opportunities related to malicious insider threats to U.S. critical infrastructure over the next 20 years. The alternative futures are not intended to predict the future but to examine plausible combinations of uncertainties and contributing factors that tell a series of compelling stories about the nature and mitigation of the insider threat.

Participants selected two major uncertainties, **governance** and **insider capabilities**, as the drivers for the alternative futures related to insider risk to the 16 U.S critical infrastructure sectors.

Two of the resulting scenarios, designated Advantage Good Guys (Traditional Insider Capabilities—Effective Governance) and Mission Impossible (Technologically-Enhanced Insider Capabilities—Haphazard Governance), present the most compelling challenges for U.S. critical infrastructure stakeholders in the combination of uncertainties and variables highlighted.

- In the Advantage Good Guys future, the traditional insider must work hard and risk exposure to identify and target what is *not* guarded in his or her domain to be successful. Effective governance creates a higher probability of detection, greatly reducing the

overall risk of an insider attack. In this world, insider collusion may become an imperative to overcome layered defenses with more physical and cyber threat mitigation controls in place.

- In the Mission Impossible scenario, the insider is more capable with enhanced tradecraft than ever before, making effective risk management more difficult, if not impossible. A non-standardized culture of governance sets the scene for repeatable and systemic attacks by insiders using technologically enhanced techniques to launch targeted and potentially widespread attacks from one or multiple vectors with minimal risk of attribution. Insiders who have worked their way up the company chain may have played a role in building the haphazard governance and infrastructure they seek to exploit. Outsourcing continually broadens the field of potential adversaries in the U.S. critical infrastructure virtual supply chain. The "high-tech" insiders have a significantly enhanced asymmetric capability to create widespread kinetic impact though cyber means. Perhaps more highly destructive is their ability to conduct widespread cyber exploitation attacks, the effects of which cannot be seen before potentially catastrophic consequences result.

Key trends that will affect the future insider threat landscape over the next 20 years include the continued viability of traditional, "low-tech" insider techniques to exploit gaps in the prevailing security environment, migration to and dependence upon the "cloud," increased potential for blended (cyber and physical) attacks, globalization, and outsourcing. These latter trends increasingly will force owners and operators to collaborate and exchange data via external/third party IT networks over whose security they have little to no control.

Risk Mitigation

Existing best practices should inform mitigation measures, but the nature of the insider threat leads to specific areas that are particularly challenging, and in which there are opportunities to strengthen current measures against malicious insiders. During the tabletop exercises and the Alternative Futures workshop in support of the NRE, subject matter experts identified the following issues as particularly challenging for insider risk mitigation:

- Acknowledging and dealing with a pervasive threat;
- Breaching roadblocks to public-private cooperation and information sharing;
- Establishing workforce behavioral and access baselines;
- Implementing effective employee insider threat training programs;
- Incorporating public information campaigns into response and recovery;
- Refining incident response to contain technically adept insiders; and
- Understanding the psychology of a malicious insider.

The research and subject matter expert elicitations supporting this NRE revealed a series of high-level key findings and themes regarding the current and future risk associated with malicious insiders across all 16 U.S. critical infrastructure sectors. This overview of the major findings and recommendations related to the malicious insider threat and owner and operator vulnerabilities provides stakeholders and policymakers with a better understanding of the scope of the threat as they develop and enhance insider mitigation policies and programs to counter it.

The Threat: Malicious Insiders

- **Access and specialized knowledge give insiders tactical advantages over security efforts.** All malicious insiders enjoy some degree of tactical advantage that owners and operators must take into account when attempting to quantify and mitigate insider risk to their organizations. They represent a special category of concern because their trusted position allows them to circumvent many of the organization's defenses, which are typically at the perimeter and directed outward. They operate with at least a minimal degree of target access and knowledge. Depending upon the scope of their access, skill level, and ability to operate with stealth–by virtue of legitimate access or deliberate action–trusted employees determined to cause harm will have overcome most hurdles that the external adversary faces in breaching the physical, cyber, and personnel-related perimeters of a targeted critical infrastructure asset. In the absence of legal, standardized, and enforceable behavioral and online monitoring protocols for current employees and trusted business partners, to include pre- and post-termination risk mitigation procedures, the threat will continue to grow.
- **Technological advances, globalization, and outsourcing increasingly blur the line between traditional insiders and external adversaries.** The boundaries of critical infrastructure, as defined today, will continue to expand to include new technologies and industries that will create new vulnerabilities. Globalization and outsourcing increasingly are "deperimeterizing"[11] U.S. critical infrastructure and broadening the field of potential adversaries in the supporting virtual supply chain. New ambiguities arise in defining insider threat boundaries that will increase potential vulnerabilities. Major drivers of this ambiguity are the economic and technological imperatives transforming critical assets from traditionally stand-alone, siloed systems into IP-based networks. Increased trust in the "cloud"[12] and Web 3.0[13] will exacerbate the problem if these technologies are not treated and protected as critical infrastructure. The risks may be particularly acute in the Banking and Finance, Information Technology, Communications, and Energy Sectors, as well as in the increasing number of control systems (including the Supervisory Control and Data Acquisition (SCADA) systems) that connect to the Internet.
- **Insiders who combine advanced technological understanding with traditional espionage/terrorist skills have a significantly increased asymmetric capability to**

[11] Deperimeterization is a termed coined by the Jericho Forum to describe the erosion of the traditional 'secure' perimeters, or 'network boundaries,' as mediators of trust and security. These boundaries are not just physical, they are also logical in the sense that they demarcate the edges of an organization or enterprise. See Dubrawsky, Ida, "The "De-perimeterization of Networks," *Microsoft TechNet*, September 12, 2007, http://technet.microsoft.com/en-us/library/cc512604.aspx, accessed September 10, 2012.

[12] "Cloud" computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. See National Institute of Standards and Technology (NIST), *The NIST Definition of Cloud Computing*, September 2011.

[13] Web 3.0 is the next stage of the Internet, an Internet for machines where everything with an electric current running through it has an IP address and is communicating with other machines like it, without the need for human intervention. This is big data, driven by the "cloud" and with the mobile device as your personally tailored endpoint that gathers, stores, accesses, and transfers this information. See Kellermann, Tom, "Evolution of Targeted Attacks in a Web 3.0 World," Trend Micro, July 2, 2012, http://cloud.trendmicro.com/the-evolution-of-targeted-attacks-in-a-web-3-0-world/, accessed August 13, 2012.

cause physical damage through cyber means. Highly cyber-skilled malicious insiders have a significantly enhanced asymmetric capability to create widespread kinetic impact though cyber means. Advances in information technology and increased dependence on the Internet offer malicious insiders converged or expanded capabilities to conduct targeted physical sabotage using cyber systems. These blended attacks at the points where physical and virtual worlds converge could have severe implications for operations and security across all 16 U.S. critical infrastructure sectors.

The Vulnerabilities: Expanding Organizational Security Boundaries

- **Even sectors with relatively robust preventative programs and guidelines in place face a dynamic and expanding threat that cannot be eliminated altogether.** Available research, data, and analysis suggest that no U.S. critical infrastructure sector, industry, or asset is immune to insider threat. The threat varies from sector to sector and from asset to asset within each sector. It only takes one well-placed insider to exploit either known vulnerabilities or "zero-day" vulnerabilities (which they may have created) within an organization to undermine the integrity of a targeted infrastructure.
- **Organizations are likely underestimating the threat from third-party insiders such as vendors and contractors.** Even though employees statistically remain the primary perpetrators of malicious insider activity, most organizations continue to underestimate the ability of unvetted third-party vendors, contractors, and trusted business partners to exploit the access credentials and privileges they have to critical facilities, systems, databases, and supply chains. [14] An increasing number of enterprises now operate as virtual amalgamations of people and systems working inside and outside the "brick and mortar" of a facility, and more and more insider cases are appearing in which the insider is a trusted business partner rather than an employee. Advanced technology increasingly blurs the line between the physical and "virtual" insider. Relatively low levels of oversight, high degrees of anonymity, and the lack of rigorous, enforceable standards for software development, manufacturing, and validation should be major concerns for the U.S. critical infrastructure community, particularly with the gradual migration from analog to digital control systems and with the migration from private data centers to hybrid and public environments.
- **Industrial control systems in major critical infrastructure sectors are attractive insider targets for remote sabotage and espionage in an increasingly networked world.** Cyber vulnerabilities exist within industrial control systems (ICS), including SCADA systems, that monitor and control equipment and physical processes in industrial and manufacturing facilities and across major critical infrastructures. ICS are attractive targets in an increasingly networked world, especially because attacks against them can be executed remotely. The subject matter experts supporting this NRE indicated that a long-term, well-orchestrated foreign nation-state espionage effort leveraging insiders to collect information on SCADA systems located in critical infrastructure is well within the realm of possibility. Such a reconnaissance campaign would be comparable to other

[14] Shaw, Eric, Ph.D, Kevin G. Ruby, and Jerrold M. Post, M.D., "The Insider Threat to Information Systems: The Psychology of the Dangerous Insider," *Security Awareness Bulletin* (No. 2-98), 1998, www.pol-psych.com/sab.pdf, accessed June 4, 2012.

types of intelligence gathering performed in support of potential military action. In addition, malicious insiders and foreign adversaries could gain an advantage by including back-up command and control systems and software in their cyberattack plans to complicate or prevent recovery efforts. Adversaries may attempt to acquire continuity of operations plans through espionage to inform an attack.

- **Without credible and sector-specific insider risk information, critical infrastructure owners and operators are likely to underestimate the malicious insider threat and make insufficient or misdirected investments in security.** In the final analysis, owners and operators of critical infrastructure must be able to make a business case for investments in reducing risk to acceptable levels. All owners and operators of U.S. critical infrastructure, both public and private, must balance operating costs against return in terms of increased security. The experts supporting the NRE observed that the public and private sectors embody different security cultures. They noted that the private sector would be reluctant to accept government-imposed standards that they perceive as requiring invasive and prescriptive vetting, hiring, and network and behavioral monitoring policies for employees of critical infrastructure and associated systems. In order to shift the policies of privately-owned infrastructure away from using minimum cost-effective standards toward implementing best practices and applying a more risk-based lens to insider threats, the experts suggested that a combination of regulation and market incentives may be required.

The Consequences: Asymmetric Impacts

- **If the goal of malicious insider activity is exploitation rather than near term destruction of assets, it will be more difficult to detect, potentially resulting in serious cumulative consequences.** Total destruction is not always the malicious insider's intent. Attacks on critical infrastructure involving the cooption of insiders often focus on exploiting a functioning system rather than simply destroying critical nodes for ideological and symbolic purposes. These types of attacks often involve systemic corruption throughout a particular infrastructure, or they simply result from one or several individuals seeking personal gain. At some point, these attacks reach a tipping point where the exploitation causes significant financial or psychological damage or severely erodes public confidence in the system.
- **The impacts of a cyberattack that is designed to cause physical damage to critical infrastructure could be much more severe than those of a conventional cyberattack.** Advances in information technology and increasing dependence upon the Internet offer future malicious insiders converged capabilities to conduct targeted physical sabotage through cyber tactics. These blended attacks where the physical and virtual worlds converge have potentially severe implications for operations and security across all 16 critical infrastructure sectors.

Recommendations

The U.S. critical infrastructure community faces both challenges and opportunities in mitigating current and future threats from malicious insiders. Existing best practices inform mitigation measures, but the nature of the insider threat leads to specific areas that are particularly

challenging, and in which there are opportunities to strengthen current measures against malicious insiders.

The need to develop and enforce a comprehensive, scalable, and cost-effective insider threat program standard for U.S. critical infrastructure was an overarching point of agreement among the subject matter experts supporting this NRE because cross-cutting standards for insider threat programs and initiatives do not exist for all sectors. While subject matter experts praised the Nuclear Sector and Electricity Sub-sector as having insider threat programs others could and should emulate, they emphasized that no sector, industry, or asset is immune to insider threats. Even sectors with relatively robust preventative programs and guidelines in place face a dynamic and expanding threat. Insider threat programs need to include monitoring, validation, and enforcement mechanisms to ensure their relevancy and effectiveness in the current threat environment.

During the tabletop exercises and the Alternative Futures workshop in support of the NRE, subject matter experts identified the following issues as particularly challenging for insider risk mitigation:

- Acknowledging and dealing with a pervasive threat;
- Breaching roadblocks to public-private cooperation and information sharing;
- Establishing workforce behavioral and access baselines;
- Implementing effective employee insider threat training programs;
- Incorporating Public Information campaigns into response and recovery;
- Refining incident response to contain technically adept insiders; and
- Understanding the psychology of a malicious insider.

Other specific mitigation recommendations that emerged from the analysis included:

- **Effective prevention and mitigation programs must be driven by better understanding the insider's definition of success against a particular sector.** Insiders will continue to use the most expedient and effective methods for opportunistic attacks against targets that are the easiest to access but not necessarily the most high-consequence in and of themselves. The terrorist insiders' intent may be to use their access and knowledge to threaten or perpetrate an attack against a strategic or political opponent/employer that discredits the industry, erodes confidence in the government, and causes mass fear and distrust. Regardless of our level of confidence in the efficacy of current safeguards, malicious insiders may be unsuccessful in inflicting catastrophic physical damage but may have other ways of defining "success" when planning or executing attacks against the most hardened sectors.
- **Organizations should establish workforce behavioral and access baselines, including an understanding of hiring, oversight, access, and security policies, in order to identify anomalies.** Organizations cannot identify anomalies if they are not familiar with normal behavior patterns for their employees. Despite this, owners and operators may use technological tools or even create standards without a comprehensive understanding of what abnormal activity looks like within their specific areas of responsibility. A critical component of filling this gap would be to recruit and leverage the expertise of

human behavioral specialists. Establishing workforce baselines requires knowledge of the workforce, including an understanding of current levels of oversight for different types of employees, and an understanding of physical and data access provisions and controls.

- **Employees used as a monitoring force may be the best way to identify malicious insiders, and they must have access to recurring training to do so effectively.**[15] Co-workers have the closest day-to-day contact with employees who may have malicious intent or who may be dealing with personal or professional issues that put them at risk. Human Resources personnel can be particularly vital sources of information because they work with an employee throughout their employment life cycle and because they are the first and last people to deal with an employee, enabling them to recognize potential for malicious behavior during employment or after termination.[16] The subject matter experts did note that turning the workforce into behavioral monitors could present significant challenges, especially in tight-knit organizations, where reporting anomalies could be seen as disloyal to colleagues.
- **Public and private organizations must consider how to balance the best risk-based security procedures against the myriad of policy, legal, and employees' rights issues associated with obtaining and analyzing relevant threat data in the workplace, especially data derived from social media and behavioral monitoring.** Highly effective insider threat programs should incorporate on-the-job behavioral analysis tools in addition to other physical security and technical solutions. Both public and private organizations must assess the best risk-based security procedures that respect employee privacy, a process that will test the limits of effective governance and constitutional rights in an increasingly digital world. One major hurdle remains overcoming the myriad of policy, legal, and employees' rights issues associated with obtaining and analyzing relevant threat data in the workplace, especially data derived from social media and behavioral monitoring. To be mindful of employee morale and mission productivity, owners and operators face the delicate task of handling security imperatives without creating an oppressive workplace environment.

[15] Gelles, Michael, David Brant, and Brain Geffert, *Building a Secure Workforce*. Deloitte Consulting LLP, 2008: 10, www.deloitte.com/view/en_US/us/Industries/US-federal-government/764ef33b4010e110VgnVCM100000ba42f00aRCRD.htm, accessed April 25, 2012.

[16] Gelles, Michael, David Brant, and Brain Geffert, *Building a Secure Workforce*. Deloitte Consulting LLP, 2008: 11, www.deloitte.com/view/en_US/us/Industries/US-federal-government/764ef33b4010e110VgnVCM100000ba42f00aRCRD.htm, accessed April 25, 2012

Chapter 3: Current Risk to U.S. Critical Infrastructure from Insider Threat

Introduction

This chapter presents the DHS findings from a risk assessment for 31 insider threat scenarios with national-level consequences. In line with the high-level scope of this NRE, this assessment focuses only on scenarios that could result in high-to-catastrophic consequences with potentially broad-reaching disruptions beyond the targeted infrastructure to other sectors. A sampling of the highest risk and consequence scenarios is included to give owners, operators, and policymakers responsible for protecting our nationally critical assets a better understanding of the categories of risk represented by trusted insiders, in order to inform mitigation policies and programs.

Summary of Methodology

The scenario-based risk assessment approach, applied to 31 insider threat scenarios with national-level consequences, reflects the high-level scope of the NRE and the nature of the supporting data. Figure 1 provides a simplified representation of the insider threat risk assessment methodology, which is addressed in detail in Appendix C.

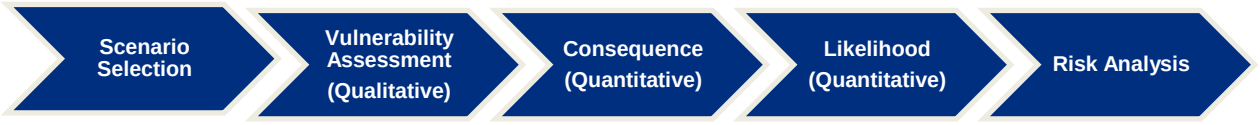

Figure 1. Insider Threat Risk Assessment Methodology

Scoping the Definition of a Malicious Insider

The analysis focuses on insiders who have an established level of trust within an organization that allows them varying levels of access or proximity to and knowledge of systems, facilities, or information associated with an infrastructure's vulnerabilities and protective security programs. As such, the analysis excludes hackers (individuals or groups) who gain unauthorized access to systems remotely via cyber intrusion. However, this analysis does include former employees and third-party or trusted business partners such as contractors, consultants, temps, students, and service/IT vendors supporting a critical infrastructure.[17] Former employees retain knowledge and may retain access directly through "back doors" or indirectly through former colleagues.

Scenario Selection

An initial set of scenarios was developed from a literature review and from open source research across each of the 16 critical infrastructure sectors. During the scenario development phase, three insider attack themes were identified–terrorism, espionage, and corruption/crime. For purposes of this risk assessment, terrorism scenarios include physical attacks and cyberattacks

[17] The CMU-SEI CERT defines a trusted business partner as "any external organization or individual an organization has contracted to perform a service for the organization. The nature of this service requires the organization to provide the trusted business partner authorized access to proprietary data, critical files, and/or internal infrastructure."

against critical infrastructure, espionage scenarios include both economic and industrial espionage, and corruption scenarios involve crime, bribery of public officials, or fraud to facilitate hostile or criminal activities including but not limited to drug smuggling, immigration, or use of taxpayer dollars. The 31 scenarios with "high" or "catastrophic" consequences of national significance were selected for use in this scenario-based risk assessment (Table 1 at the end of the next section). These scenarios are a representative sample of potential insider attacks and are not a comprehensive set.

Consequence Assessment

"Consequence" represents the expected adverse impact from an attack. The consequence estimate for each scenario is based on the worst reasonable impact of the scenario. The 31 scenarios used in the risk assessment include four with catastrophic consequences and the remaining 27 scenarios with high consequences.

Likelihood

"Likelihood" is defined as the estimated relative frequency of a specific insider scenario occurring relative to the set of scenarios. The range of likelihood estimates for many of the scenarios is substantial due to the inherent uncertainty in the available data.[18]

Overview of General Insider Risk Assessment Categories

Analysis of the risk assessment results for the NRE scenario set revealed three broad risk categories that help characterize the distribution of insiders and the chosen attack methods within the likelihood-consequence spectrum. Ultimately, these categories reflect commonalities within the four likelihood-consequence quadrants (Figure 2) that are defined by varying degrees of malicious insider access levels, technical and specialized skills, positional authority, and job autonomy as well as the robustness of the targeted infrastructures or supporting assets. Figure 2 displays the 31 insider threat scenarios with consequences of national significance and indicates the type of attack and scenario reference number for each scenario. Table 1 at the end of this section provides a description of each scenario with the reference numbers as displayed in Figure 2.

Following is a brief overview of the three identified risk categories.

[18] Appendix C on Risk Assessment Methodology, especially Figure C-4 and associated text, addresses the uncertainty in the available data.

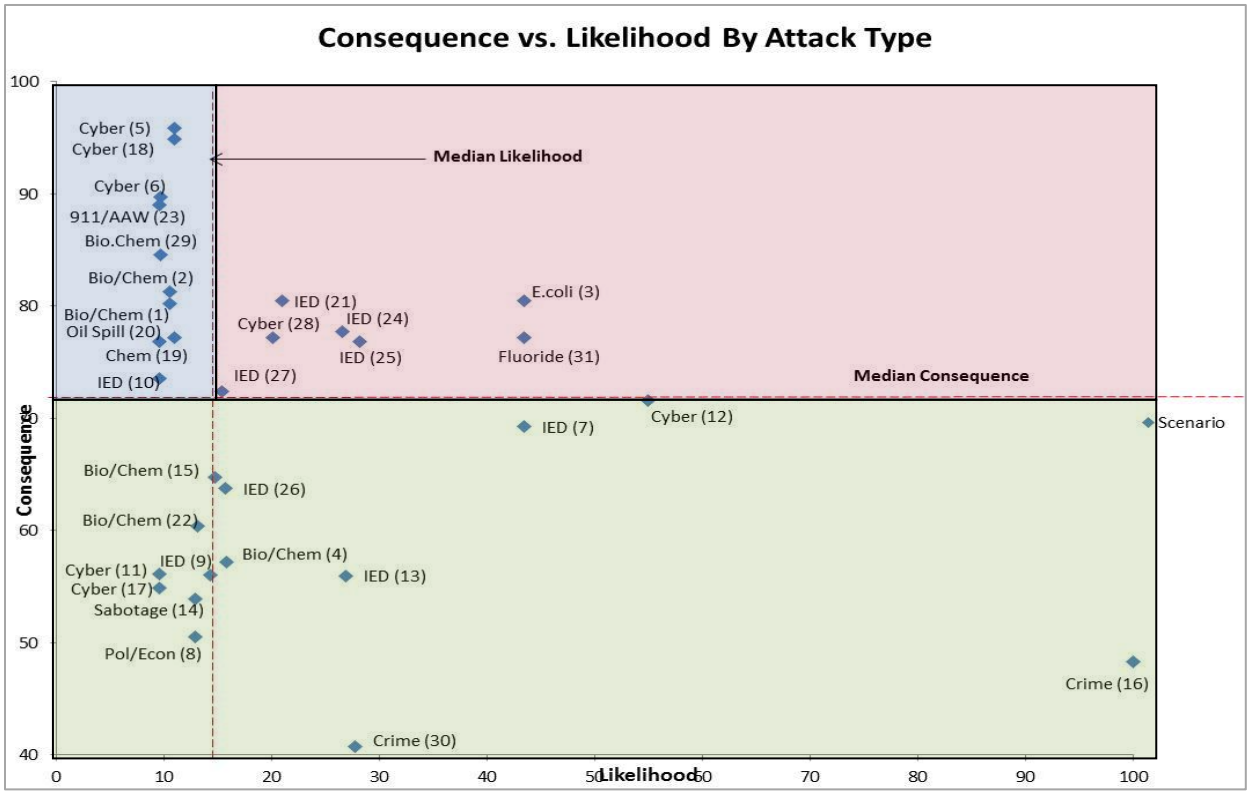

Figure 2. Relative Risk Analysis by Attack Type

Medium- to High- Likelihood and High- to Catastrophic-Consequence Attacks (shaded in red in Figure 2). Most of the attack scenarios in the medium- to high-likelihood and high- to catastrophic-consequence region tend to be relatively low-cost, "low-tech," kinetic, and /or *opportunistic* in nature against a target's known vulnerabilities. In many cases, these attacks could easily be executed by non-insiders who acquire general knowledge about the target. General characteristics of the malicious insiders and their targets in this quadrant include:

- The insider is a lower-skilled, perhaps even an entry-level employee, with little to no supervisory authority, and limited financial or material resources;
- The insider has only general access required to perform his or her job with little or no privileged access to the most critical systems or assets;
- The insider is likely to exploit access to specific area(s) to conduct an attack, especially if he or she happens to have knowledge of target vulnerabilities such as work schedules/shifts and infrastructure weaknesses; and
- The targeted infrastructure or supporting asset tends to have less robust personnel, physical, and cybersecurity programs in place.

Low-Likelihood and High- to Catastrophic-Consequence Attacks (shaded in blue in Figure 2). The attack scenarios in the low-likelihood and high- to catastrophic-consequence quadrant are best categorized as the "worst nightmare" scenarios that pit the highly motivated and highly skilled insiders against some of the most robust and well-defended critical infrastructure facilities and supporting assets in the Nation. To be successful, the attacks tend to be highly technical,

complex, and *targeted* against known or previously unknown (zero-day) vulnerabilities. The more complex and severe attacks may involve substantial collusion or financial resources from outside adversaries who exploit well-placed insiders as force multipliers. General characteristics of the malicious insiders and their targets in this quadrant include:

- The insider tends to be highly-skilled, experienced, or specialized;
- The insider tends to enjoy moderate to generous levels of job autonomy by virtue of their supervisory position and level of skill;
- The insider may have access to a moderate level of financial or material resources;
- The insider is likely to have faced relatively tight hiring requirements;
- The insider holds specialized or highly privileged access to critical systems or assets;
- The insider uses technically sophisticated attacks with high cyber content;
- The insider is more likely to participate in sabotage through cyberattacks or exploitation, to include writing or delivering malicious code or disrupting critical components in the supply chain; and
- The attacks would be extremely difficult for outsiders to execute successfully without insider collusion or the involvement of an unwitting insider.

Low- to High-Likelihood and Medium-High- to High-Consequence Attacks (shaded in green in Figure 2). The attack scenarios in the low- to high-likelihood and medium-high- to high-consequence region, although serious, tend to fall into the corruption and exploitation categories or represent versions of more serious attacks that involve insiders who have malicious intent when they apply for employment and must overcome screening hurdles before committing their malicious attacks. In addition, some of the attack scenarios involve cybercrime. As with the high likelihood and high- to catastrophic-consequence scenarios, many of these attacks could be carried out by insiders or outsiders who acquire general knowledge about the target.

Table 1. Scenarios Used for Insider Threat Risk Assessment

No.	Sector	Scenario Description
1	Food and Agriculture	Terrorism: An insider contaminates food processing plant via biological attack by introducing toxin into the U.S. milk supply. A 2005 Stanford University study pointed out that the milk industry's distribution systems are vulnerable to bioterrorism through the introduction of botulinum toxin, a deadly poison, into the milk supply. Based on the contamination of a single milk tanker and milk-processing facility, the toxin could be introduced to a large supply of milk via centralized storage and processing. This would dilute the toxin throughout several thousand gallons of milk and lead to widespread consequences.
2	Food and Agriculture	Terrorism: An insider contaminates food processing plant by introducing toxic chemical into the U.S. milk supply. Scenario No. 1 used as proxy for judgments on this scenario No. 2
3	Food and Agriculture	Terrorism: An insider contaminates beef in meat packing plant with E. coli O157 to create loss of confidence in food supply and nation-wide panic.

No.	Sector	Scenario Description
4	Food and Agriculture	Terrorism: An employee at a foot and mouth disease (FMD) biological-research center in the United States decides to circumvent on-site biosecurity measures to remove live FMD serotype from the facility and introduce it to multiple livestock feedlots and transport nodes in the U.S. "beef belt." This scenario has significant impact on the U.S. beef industry because of the specific serotype; the time elapsed from confirmation of the serotype, the number of animals exposed, and the push for emergency vaccinations.
5	Financial Services	Terrorism, Espionage, Corruption: An insider recruited by a foreign power or criminal organization to conduct cyberattack on an international financial system to disrupt international financial transactions and terrorist financial tracking
6	Financial Services	Terrorism, Corruption: A foreign organized crime group with links to a hostile nation-state coerces a financial clearing house employee, either on the software development or vulnerability management team, to attack the clearing house with the goal of creating massive capital flight from the United States. An insider interfering with time stamps on high-frequency trades could create a sudden liquidity crisis and a potential mini-market crash, thus having a potentially catastrophic impact on the U.S. economy.
7	Commercial Facilities	Terrorism: A disgruntled employee comes under influence of an outside terrorist organization and/or self-radicalizes. The employee learns that he or she will be let go by the company and decides to detonate a Vehicle-Born Improvised Explosive Device (VBIED) against the employer's place of business.
8	Communications	Terrorism: Insiders disrupt supply chain flow of Rare Earth Elements (REEs), which are critical components in cell phones and microwave and satellite communication systems. Insiders instigate political or trade disputes in the country of origin so that that nation purposely reduces or bans exports; or instigate labor strikes that halt the mining and processing of REEs. In 2008 a single foreign country supplied 96 percent of the U.S. imports of REEs; such a disruption in that country could potentially have significant consequences for the Communications Sector.
9	Critical Manufacturing	Terrorism: An insider at a major U.S. maritime port plants a powerful bomb that temporarily closes the port and the effects are felt throughout the CM Sector supply chain. U.S. maritime ports handle two billion tons of domestic and foreign cargo every year. The Critical Manufacturing (CM) Sector, in particular, relies on maritime ports for the import of raw materials, components, and finished products.
10	Dams	Terrorism: A disgruntled employee comes under influence of an outside terrorist organization and/or self-radicalizes. Employee learns he or she is going to be let go by the company and decides to detonate a large Improvised Explosive Device (IED) against a critical point in the dam's facility.
11	Energy	Terrorism: A foreign nation-state recruits an insider sympathetic to the foreign nation to carry out a sophisticated cyberattack on the automated control systems of a U.S. electrical transmission line.
12	Energy	Terrorism, Industrial Espionage: A foreign entity recruits an insider to provide essential information to enable them to engineer their hardware and embedded software products so that, once installed, they provide a “back door” for capturing and mapping real-time U.S. SCADA and “smart grid” system data. The information gained could be used to disrupt the system in time of conflict.
13	Government Facilities	Terrorism: A disgruntled employee comes under influence of an outside terrorist organization and/or self-radicalizes. The employee learns that he or she is going to be let go by the government and decides to detonate a VBIED against their employer's place of business.

No.	Sector	Scenario Description
14	Healthcare and Public Health	Terrorism, Corruption, Espionage: An insider disrupts supply chain flow of critical raw materials for health care equipment. Medical products and services rely on advanced technologies, such as nuclear technologies, that use rare raw materials from only a few suppliers. For example, the global isotope supply chain depends on a small number of aging nuclear reactors for isotope production and a complex processing and distribution chain for delivery of short-lived isotope products to the health care system. A disruption of the supply of the isotope Mo-99 could have significant impact on the global medical supply chain.
15	Healthcare and Public Health	Terrorism: Insider contaminates materials used in pharmaceutical production in an area that has a high concentration of pharmaceutical facilities. This disruption has a devastating effect on the U.S. supply of pharmaceuticals.
16	Healthcare and Public Health	Corruption/Organized Crime: A foreign-based organized crime organization uses insiders to facilitate its Medicare and Medicaid fraud activities in metropolitan centers in at least 20 States. This multinational criminal organization (MCO) is using traditional approaches including creating service providers and sham storefronts, etc. The MCO has recruited or placed insiders in a few major hospitals in the region, in regional Medicare Administrative Contractors, and in Centers for Medicare and Medicaid Services who are involved in claims and billing systems or who can facilitate processing fraudulent claims.
17	Information Technology	Terrorism: A foreign nation-state recruits an insider (with malicious intent after being hired) sympathetic to the foreign nation to attack U.S. electrical transmission lines.
18	Information Technology	Terrorism, Espionage, Corruption: Insider recruited by foreign power or criminal organization to conduct a cyberattack on an international financial system to disrupt international financial transactions and terrorist financial tracking.
19	Chemical and Transportation Systems	Terrorism: A foreign-based criminal organization recruits a criminal alien to detonate a truck containing chlorine inside a tunnel of a major metropolitan area.
20	Energy	Terrorism: A disgruntled employee causes an explosion on an offshore drilling rig in the Gulf of Mexico, resulting in the deaths of several workers, sinking of the drilling unit, an oil spill lasting three months, and various other economic, ecological, and health-related consequences.
21	Transportation Systems	Terrorism: A postal worker who is going to lose his or her job due to cutbacks at U.S. Postal Service (USPS) decides to get even with his employer by introducing an IED into the mail system. The worker has extensive knowledge of USPS air mail handling procedures and is able to circumvent existing countermeasures.
22	Transportation Systems	Terrorism, Corruption: A postal employee is recruited or coerced by an outside terrorist organization to introduce a biological agent into a postal facility. The employee receives financial rewards in exchange for his or her participation.
23	Transportation Systems	Terrorism: An airline pilot going through difficult personal time (e.g., financial troubles, divorce with intense custody battle) decides to deliberately crash the plane into a critical infrastructure asset.
24	Transportation Systems	Terrorism, Corruption: A baggage handler is a willing participant in a drug smuggling ring and had previously placed packaged thought to be carrying illegal drugs into the cargo hold of passenger aircraft. Unbeknownst to the baggage handler, the drug smuggling handlers are actually terrorists who eventually swap an explosive or bomb-making components for the "drug package" which then is placed in the cargo hold and detonated, resulting in the catastrophic loss of the aircraft.
25	Transportation Systems	Terrorism, Corruption: An airport screener is a willing participant in a drug smuggling ring and had previously allowed persons carrying drugs to pass through security checkpoints. Unbeknownst to the screener, the drug smuggling handlers are actually terrorists who eventually swap an explosive or bomb making components for the supposed drug package which then is allowed onto a passenger aircraft and results in the catastrophic loss of the aircraft.
26	Transportation Systems	Corruption: For financial gain, a field maintenance worker places an IED on section of pipeline to cause a double shear of pipe in a very remote location.

No.	Sector	Scenario Description
27	Transportation Systems	Terrorism: A disgruntled railroad employee with access to key bridges (e.g., maintenance worker, or mechanical engineer) deliberately causes mechanical failure at key vulnerable locations on railroad bridges.
28	Transportation Systems	Terrorism: A foreign nation recruits multiple insiders to conduct integrity attacks on rail control centers SCADA/scheduling systems (and other vectors) to delay U.S. military movement.
29	Transportation Systems	Terrorism: A terrorist group recruits an insider to assist with their successful wide-area biological/chemical attack on a major U.S. port. The attack kills or incapacitates the majority of the port's workforce and cripples the port's petrochemical complex and significantly disrupts the petrochemical industry. In addition, the port is closed for an indeterminate length of time, having a severe impact on its economic activity.
30	Border Security	Corruption: A drug cartel near the Southwest border of the United States recruits insiders who have access at border and operating nodes to facilitate expanding influence in United States, in order to gain access to rival group's territory and financial resources.
31	Water and Wastewater Systems	Terrorism: Terrorist group recruits insiders to inject lethal levels of fluoride into a municipal water treatment plant along the U.S. East Coast to disrupt the drinking water supply and to create panic.

The Complex Nature of the Insider Adversary as It Affects Risk

A Far-Reaching Threat

The available data and research confirm that no critical infrastructure sector, industry, or asset is immune to the full scope of insider threats. Even with preventative programs and guidelines in place, the insider threat is a dynamic and expanding one that cannot be eliminated altogether. As highlighted in a seminal 2009 study by Carnegie Mellon Software Engineering Institute (CMU-SEI CERT) and emphasized repeatedly by subject matter experts in the workshops and tabletop exercises for this NRE, the scope of insider threats goes well beyond those posed by current and former employees of critical infrastructure.[19] As the CMU study indicates and as many other analyses suggest, factors such as cyber technology, globalization, outsourcing, multiculturalism, and divided loyalties complicate the insider threat problem for infrastructure owners and operators. All of these blur the line between traditional insiders and external adversaries such as terrorists, organized crime groups, and foreign nation-states, who may collude with or exploit physical insiders as vectors to do harm to a targeted asset or system.[20] The assessment process is further complicated by the overall dearth of detailed empirical data on malicious insider activities, particularly in the non-IT/non-data breach realms, and by the ongoing research challenge of trying to understand and quantify the "human factors" and psychology associated with potential insider actors.

[19] Cappelli, Dawn, Andrew Moore, Randall Trzeciak, and Timothy J. Shimeall, *Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition – Version 3.1,* Carnegie Mellon University (CMU)-Software Engineering Institute (SEI) CERT, January 2009: 6.

[20] According to CMU-SEI CERT findings, approximately half of the insiders who stole or modified information for financial gain were recruited by outsiders, to include organized crime and foreign organizations or governments. See Cappelli, Dawn, Andrew Moore, Randall Trzeciak, and Timothy J. Shimeall, *Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition – Version 3.1,* Carnegie Mellon University (CMU)-Software Engineering Institute (SEI) CERT, January 2009: 6.

The fundamental challenge with malicious insiders is that they understand an organization's vulnerabilities first-hand. They present a special category of organizational concern because their trusted position allows them to circumvent many of the institution's defenses, which typically are directed outward. Whether a malicious insider actually perpetrates or simply facilitates an attack, his or her level of access to and knowledge of the targeted facility, asset, and/or associated data and systems are critical to assessing the likelihood and consequences of the attack. Trying to defend against the well-placed, savvy insider easily could create a workplace environment that impedes operational processes.

When the Insider and External Threat Actor Merge

Several recent assessments, as well as the comments from subject matter experts supporting this NRE, suggest that the collusion of malicious insiders— including third-parties—with well-resourced, sophisticated foreign nation-state or other high-level adversaries may represent the most serious and damaging threat to U.S. critical infrastructure either in the form of espionage, kinetic, or cyber sabotage.

According to CMU-SEI CERT's data analysis, approximately half of the insiders who stole or modified information for financial gain are recruited by outsiders, to include organized crime groups and foreign organizations or governments.[a]

The use of insiders as force multipliers to facilitate external cyberattacks is of particular concern. The 2012 final report by the North American Electric Reliability Council Cyberattack Task Force reflects this:

> **"*Insiders pose the greatest threat, especially if they are working with a Foreign State or other High level Threat Actors, because of their detailed knowledge of system operations and security practices. In addition, they have legitimate physical and electronic access to key systems and the controls designed to protect them. Insider individuals can provide qualitative, technical, or physical assistance to the team requirements of sophisticated adversaries or pose a unique unilateral threat detection challenge, if acting alone*."[b]**

[a] Cappelli, Dawn, Andrew Moore, Randall Trzeciak, and Timothy J. Shimeall, *Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition – Version 3.1,* Carnegie Mellon University-Software Engineering Institute CERT, January 2009: 6.
[b] North American Electric Reliability Council, *Cyberattack Task Force: Final Report*, May 9, 2012: 9.

Available research suggests that many organizations continue to underestimate the ability of potentially unvetted third-party vendors and trusted business partners to exploit whatever access they have to critical facilities, systems, and databases, and it demonstrates that efforts to combat malicious insider threat are not keeping pace with the threat.[21] A March 2012 Government Accountability Office (GAO) report reflects this concern specifically as it relates to contractors and service providers in the IT supply chain who may have access to Federal systems and could attempt to use that access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other systems and networks.[22]

[21] Shaw, Eric, Ph.D, Kevin G. Ruby, and Jerrold M. Post, M.D., "The Insider Threat to Information Systems: The Psychology of the Dangerous Insider," *Security Awareness Bulletin* (No. 2-98), 1998, www.pol-psych.com/sab.pdf, accessed June 4, 2012.
[22] U.S. Government Accountability Office, *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks,* GAO-12-361, Washington, D.C.: U.S. Government Accountability Office, March 2012: 15.

Just as technology increasingly blurs the line between the internal and external adversary, it also fails to differentiate between the physical and the "virtual insider" who may not share the same level of corporate loyalty as a direct employee or whose company does not abide by the same culture of security as the targeted organization. Within the cyber realm, high personnel turnover rates throughout project or contract phases, combined with an ability to operate with relatively low levels of oversight and high degrees of anonymity, increases the risk. The threat stemming from supply chain sabotage by third-party vendors and contractors was also a recurring theme discussed by subject matter experts during the workshops and tabletop exercises for this NRE. Of particular concern were software or control system vendors who have remote access credentials and maintenance privileges for critical infrastructures and associated assets.

A 2010 CMU-SEI CERT study found that employees rather than trusted business partners remain the primary perpetrators of malicious insider activity. Of roughly 300 cases in CMU's database, only 10 percent were attributed to trusted business partners with most occurring in the government (33.3 percent) and IT/telecommunications (25.0 percent) sectors. Other industry sectors heavily affected by trusted business partners included banking and finance (10.4 percent), manufacturing (12.5 percent), and medical (8.3 percent). The study notes that these numbers are not so much a reflection of increased susceptibility or vulnerability as they are of the possession of data that adversaries truly want.[23]

Advantage: Insider

No matter what their positions, identities, motivations, or triggers may be, malicious insiders share a tactical advantage in most cases, which must be taken into account when attempting to quantify risk. Insiders already operate with some degree of target access and knowledge. Depending upon the degree of their access, skill, and stealth, malicious insiders may have overcome most of the initial hurdles to breaching the physical, cyber, and personnel perimeters of a targeted asset.

Even if a critical infrastructure sector or asset has a relatively robust insider threat program in place, that program must be evaluated and tested constantly to ensure that it can keep at least one step ahead of a potentially elusive adversary. The 2010 Deloitte National Association of State Chief Information Officers (NASCIO) Cybersecurity Study reflects this perpetual concern. Only 13 percent of the Chief Information Security Officers (CISOs) surveyed were "very confident" or "extremely confident" that their organizations' information assets were protected from internal threats.[24] Only nine percent of the CISOs held the same level of confidence in the information security practices of their third-party vendors and trusted business partners.[25] These

[23] Weiland, Robert M., Andrew P. Moore, Dawn M. Cappelli, Randall F. Trzeciak, and Derrick Spooner, *Spotlight On: Insider Threat from Trusted Business Partners,* Carnegie Mellon University-Software Engineering Institute CERT, February 2010: 4.
[24] Deloitte and the National Association of State Chief Information Officers, *The 2010 Deloitte-NASCIO Cybersecurity Study,* Deloitte Development, LLC: 18, www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2010.pdf , accessed June 4, 2012.
[25] Deloitte and the National Association of State Chief Information Officers, *The 2010 Deloitte-NASCIO Cybersecurity Study,* Deloitte Development, LLC: 20, www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2010.pdf, accessed June 4, 2012.

concerns are not new; over a decade ago, a Symantec *2001 Cost of Data Breach Study* attributed 33 percent of criminal attacks against surveyed companies to malicious insiders.[26]

"People are an organization's greatest asset and most critical liability."
Deloitte Consulting LLP, "Building a Secure Workforce" (2008)

Malicious insiders, along with careless or negligent insiders who may be exploited by others, are organizational vulnerabilities – adversarial force multipliers who can operate relatively unfettered. One study refers to this as a "trust trap" that may manifest itself in any combination of an environment of excessive employee trust, reluctance to report on coworkers, and inconsistent or non-existent enforcement of organizational governance.[27] Trust in the workforce, particularly in the private sector, can have both favorable and unfavorable consequences. Employees must be entrusted with the resources, accesses, and responsibilities to perform their jobs and to keep business operating smoothly. When employees maliciously betray that trust or disregard security protocols, they create vulnerabilities that others may exploit with consequences that can be operationally and economically catastrophic.

The CMU-SEI CERT succinctly characterized the malicious insider's tactical advantage in its January 2009 *Common Sense Guide to Prevention and Detection of Insider Threats*:

> "*Insiders have a significant advantage over others who might want to harm an organization. Insiders can bypass physical and technical security measures designed to prevent unauthorized access. Mechanisms such as firewalls, intrusion detection systems, and electronic building access systems are implemented primarily to defend against external threats. However, not only are insiders aware of the policies, procedures, and technology used in their organizations, but they are also aware of their vulnerabilities, such as loosely enforced policies and procedures or exploitable technical flaws in networks or systems*."[28]

Malicious insiders are not only aware of an organization's existing weaknesses; they may have created the very system vulnerabilities and security environments they will exploit to do harm.

The Difficulty in Quantifying Unknowns

Two major factors complicate current efforts to assess the likelihood of malicious insider attacks: 1) the ongoing challenge of trying to identify and predict the stressors, triggers, and "human factors" that cause a trusted employee to cross into the realm of malicious actors, and 2) a lack of detailed empirical data on insider breaches and attacks.

Given the legitimate access and privileges that all would-be insiders enjoy, subject matter experts consulted for this NRE questioned why the United States has not experienced a significant

[26] Ponemon Institute, LLC, *2011 Cost of Data Breach Study: United States*, March 2012: 9, http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf, accessed June 12, 2012.
[27] Moore, Andrew Moore, Dawn Cappelli, and Randall Trzeciak, *The 'Big Picture' of Insider IT Sabotage Across U.S. Critical Infrastructures,"* Carnegie Mellon University-Software Engineering Institute CERT, May 2008: 10.
[28] Cappelli, Dawn, Andrew Moore, Randall Trzeciak and Timothy J. Shimeall, *Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition – Version 3.1,* Carnegie Mellon University-Software Engineering Institute CERT, January 2009: 7.

increase in insider attacks, particularly of the purely kinetic variety. Not every disgruntled, ideological, narcissistic, greedy, or financially-stressed employee with access and knowledge follows a "critical pathway" to becoming a bad actor once they are hired.[29] Existing literature and subject matter expert elicitations for this NRE tend to agree that more research and analysis is required in this area. At the same time, it is clear that there is no "one size fits all" formula for predicting malicious insider behavior, given that individuals who enter an organization with the training and intent to do harm, or those acting on behalf of a foreign nation-state or terrorist organization, would most likely have a different psychological and motivational mindset from those whose actions develop from more immediate circumstances of employment or finances.

A lack of detailed data sets available for research is an impediment to fully understanding and detecting insider threat indicators. Studies dating as far back as 1998 attribute this to a resistance or hesitancy by owners, operators, and businesses to report insider incidents for fear of publicizing their vulnerabilities or generating negative public opinion to the detriment of business continuity and profits.[30,31,32] The 2008 NIAC report discusses this in terms of the "stigma" carried by an insider betrayal, which erodes customer, partner, and shareholder trust in an organization. Consequently, owners and operators may choose to handle these types of incidents internally, quickly, and discreetly out of public view.[33] Available studies also tend to agree that many non-kinetic incidents or breaches executed by malicious insiders and trusted business partners simply go undiscovered because there are no mechanisms in place to alert an organization that something is amiss, or because the insiders are able to circumvent or disable these mechanisms. The 2012 Verizon Data Breach Investigations Report suggests that this may particularly hold true for sensitive or proprietary data compromises in the non-financial arena.[34]

The available data (which predominantly relate to cyber/IT sabotage, theft of intellectual property, and espionage) do not characterize in detail the full scope of insider threat to U.S. critical infrastructure and do little to explain why the United States has not seen more insider attacks, particularly those that could result in high-to-catastrophic consequences. They do at least provide a starting point from which to create a baseline threat profile that can be used to assess the insider threat of all types across the 16 critical infrastructure sectors.

---

[29]Shaw, Eric Ph.D, Kevin Ruby, and Jerrold M. Post, M.D., "Insider Threat to Information Systems: the Psychology of the Dangerous Insider," *Security Awareness Bulletin* (No. 2-98), 1998: 8–9, www.pol-psych.com/sab.pdf , accessed June 4, 2012.

[30] Caputo, Deanna D., Greg Stephens, Brad Stephenson, and Minna Kim, *Human Behavior, Insider Threat, and Awareness: An Empirical Study of Insider Threat Behavior*, The MITRE Corporation, July 31, 2009: 1.

[31] Shaw, Eric Ph.D, Kevin Ruby, and Jerrold M. Post, M.D., "Insider Threat to Information Systems: the Psychology of the Dangerous Insider," *Security Awareness Bulletin* (No. 2-98), 1998: 8–9, www.pol-psych.com/sab.pdf , accessed June 4, 2012.

[32] Noonan, Thomas, and Edmund Archuleta, *The National Infrastructure Advisory Council's Final Report and Recommendations on The Insider Threat to Critical Infrastructure*. Washington, D.C.: National Infrastructure Advisory Council, April 2008: 11.

[33] Noonan, Thomas, and Edmund Archuleta, *The National Infrastructure Advisory Council's Final Report and Recommendations on The Insider Threat to Critical Infrastructure*. Washington, D.C.: National Infrastructure Advisory Council, April 2008: 4.

[34] Verizon RISK Team, *2012 Data Breach Investigations Report*, Verizon, 2012:18, www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf, accessed June 4, 2012. This report was produced with cooperation from the U.S. Secret Service, the Australian Federal Police, the Dutch National High Tech Crime Unit, the Irish Reporting and Information Security Service, and the Police Central 1-Crime Unit.

Discussion of Major Insider Characteristics and Risk Categories by Quadrant

The scenarios that form the basis of the risk assessment in this NRE all result in medium-high to catastrophic consequences. The initial risk score was a simple function of the consequence and likelihood scores. A Monte Carlo simulation was conducted with the range of risk scores as the inputs for each scenario.[35] The simulation produced an expected value for risk with standard deviation. A graphical depiction of the normal distribution of risk scores with the range and 95 percent expected value box is shown in Figure 3 (see Table 1 for a description of the scenarios corresponding to the reference numbers used in Figure 3).

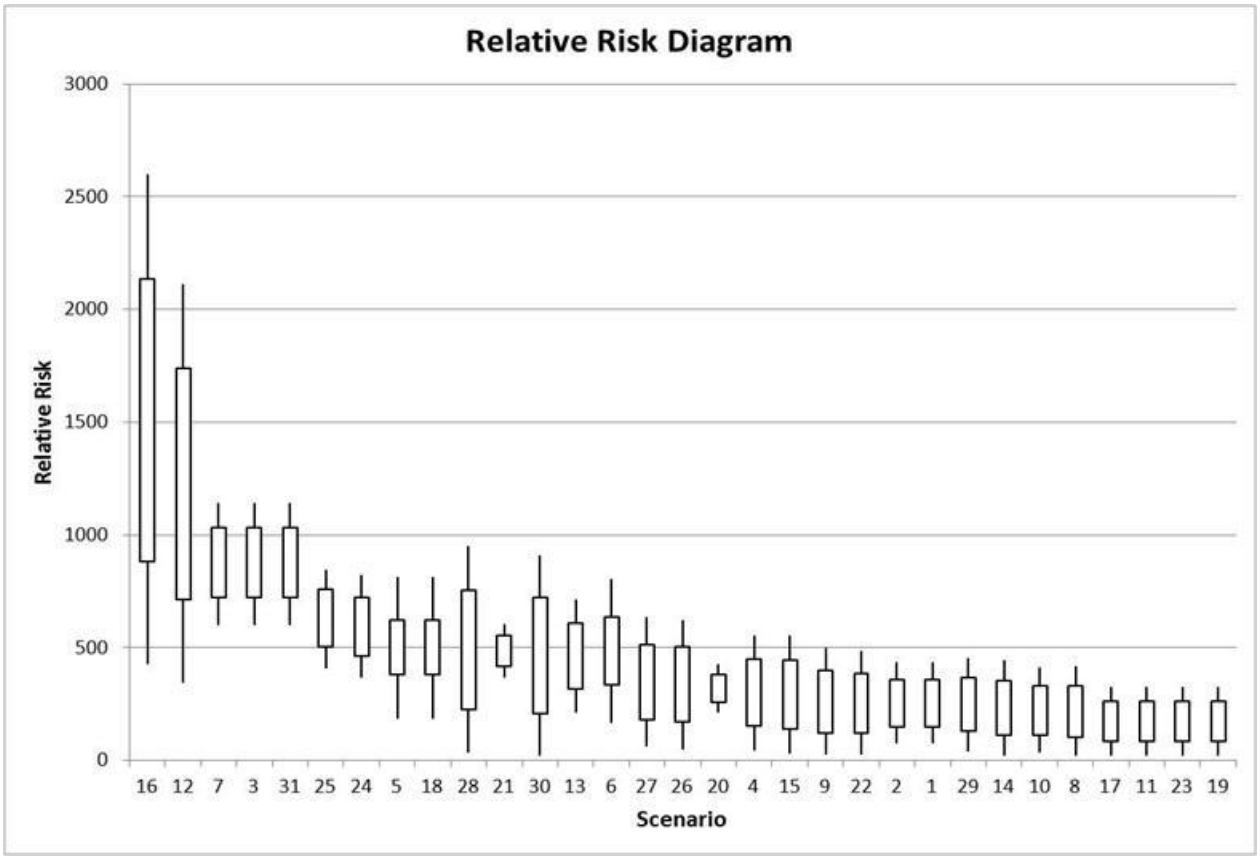

Figure 3. Relative Risk Analysis for Each Scenario from Table 1

The risk assessment rated each of the scenarios against one another and identified the relative likelihood and consequence of each scenario. This allowed placement of the relative risk of identified scenarios on a likelihood and consequence chart to reveal certain risk categories regarding attack type, attack complexity, insider access, and insider skill level (as was illustrated in Figure 2).

[35] A Monte Carlo simulation is a technique that uses random sampling of data to calculate results based on a probability distribution. It is often used to simulate mathematical models and is ideal for models with small sample sizes. Appendix C on Risk Assessment Methodology discusses the use of Monte Carlo simulation in this risk assessment.

Attack Type and Complexity

The initial identification of scenarios included three broad motivations for an insider attack– corruption, espionage, and terrorism. While these provide the reasons for an attack, the attack mode is more pertinent when evaluating relative risk. The three primary modes of attack that emerge from the risk assessment are kinetic, cyber, and exploitation attacks. The relative complexity of each attack category provides initial general parameters for the skill and access levels of the malicious insiders who are most likely to undertake them.

- *Kinetic attacks*[36] range from an insider unknowingly allowing an improvised explosive device (IED) onboard a commercial airplane to an insider actively working to cause a nuclear power plant meltdown. Kinetic attacks using IEDs are generally less complex and can be perpetrated by a single or very small group of insiders.
- *Cyberattacks*[37] that are sophisticated involve higher levels of complexity that may require the insider to have both access and knowledge of specialized computer systems and programs used by the targeted infrastructure. The more complex cyberattacks, essentially force multipliers, may require a team of insiders to coordinate the attack and to defeat all layers of countermeasures. It should be noted, however, that there is a growing criminal virtual "arms bazaar" of automated cyber capabilities which can be provided to technically unsophisticated individuals.[38]
- *Exploitation attacks*[39] on critical infrastructure exploit and work within a functioning system to achieve nefarious ends such as personal financial gain or espionage. These attacks generally are not designed to destroy any part of critical infrastructure but rather to rely on its continued operations to facilitate a criminal or terrorist operation. A single insider could perpetrate exploitation attacks, or these attacks could be part of a large-scale systemic corruption of a critical infrastructure by organized crime groups.

Insider Access and Skill Level

The type of attack roughly correlates with the skill level of the insider(s) perpetrating or facilitating the attack. A *low-skilled insider* would likely hold an entry-level position, with minimal or no supervisory authority, and possess no significantly specialized knowledge or advanced education. A *high-skilled insider* would likely hold a more technical or supervisory position. This type of insider is more likely to have specialized knowledge in their field, an

[36] As defined by the Defense Department, a kinetic attack is "one using weapons that rely on energy–blast, heat, and fragmentation, for example–to cause their damage. A non-kinetic attack might involve electronically disabling an enemy's computers and communication equipment." See Pardis, John, "Strategic Command Missions Rely on Space," September 29, 2003, www.defense.gov/news/newsarticle.aspx?id=28408, accessed July 30, 2012.
[37] As defined by the National Institute of Standards and Technology (NIST), a cyberattack is "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information." See NIST, *NIST IR 7298 Revision 1: Glossary of Key Information Security Terms*, February 2011: 56.
[38] See Goncharov, Max, *Russian Underground 101*, Trend Micro, Inc., 2012, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf, accessed December 22, 2012.
[39] For the purposes of this NRE, an exploitation attack is defined as an attack on critical infrastructure that is focused on exploiting and working within a functioning system to achieve nefarious ends rather than destroying critical nodes for ideological or symbolic purposes.

advanced degree, and some level of job autonomy.[40] The two types of insiders are likely to have different levels of access to facilities, cyber assets, and personnel in an organization. A low-skilled insider may have legitimate and minimally scrutinized physical access to a large area of a facility, which allows for extended observation or entry to sensitive areas; however, the employee is unlikely to have access to internal cyber systems, computer servers, or control rooms. This does not mean that a low-skilled insider cannot perpetrate a cyberattack, but it does mean that a low-skilled insider may be less likely to successfully perpetrate such an attack and the attack will exhibit different characteristics than those perpetrated by the high-skilled insider.

When Trust, Autonomy, and Malicious Intent Converge

A contract hospital security guard, working at night under no supervision, used his key to access a heating, ventilation and air conditioning (HVAC) computer that was housed in a locked room. As a result, he was able to remotely access that computer in addition to a nurses' workstation connected to all of the hospital's computers. Over the course of two days, the insider planted malicious code on the hospital's network that caused the HVAC system to become unstable. Had the insider not been careless enough to post video of himself planting the code, his actions could have brought down the entire HVAC system, including those elements in place to protect temperature-sensitive drugs, supplies and patients, instead of causing a short outage.

A trusted third-party employee, the security guard was part of the Internet underground and the leader of a hacking group.[a]

[a] Silowash, George, Dawn Cappelli, Andrew Moore, Randall Trzeciak, Timothy J. Shimeall and Lori Flynn, *Common Sense Guide to Mitigating Insider Threats – 4th Edition*. Carnegie Mellon University (CMU)–Software Engineering Institute (SEI) CERT, December 2012:33-34.

Insider Type and Attack Type

Analysis suggests that the insiders tend to gravitate toward, or are recruited for, specific types of attacks commensurate with their relative skill levels. *Low-skilled* insiders are more likely to take advantage of access to a specific area to conduct a physical or an exploitation attack. This could include placing a contaminant in food, using an IED to disable a critical infrastructure facility, or knowingly allowing an outside entity to use critical infrastructure systems for their own gain. *High-skilled* insiders are more likely to participate actively in a sabotage attempt through a cyberattack or an exploitation event. This could include writing malicious code and then installing that code or disrupting critical components in a supply chain. Physical attacks (including kinetic, chemical, biological, radiological, and nuclear events) generally are high-risk or high-consequence events, while cyber and exploitation events tend to have lower immediate consequences and in some cases lower likelihood. This is not necessarily the case, however, with "blended" sabotage attacks, in which a cyber-vector is used to create physical damage. For example, such an attack might be intended to alter chemical or pharmaceutical formulas or to damage or destroy industrial control systems and harm infrastructure.

[40] Note that there might be some variation in the positions held by the insider. A high-skilled insider could pose as a janitor or be forced by economic circumstances to take a job for which he or she is overqualified. Similarly, a low-skilled insider who has worked in a company for the majority of his or her career may have some significant supervisory authority over non-technical employees.

A major underlying variable that must be considered when attempting to make any correlation between insider type and attack type is the insider's willingness to be caught and punished for his or her actions. The malicious insider with no concern for personal consequences may be willing to undertake actions that differ widely from the insider wanting to avoid consequences. If an insider is willing to risk imprisonment or death, then no range or category of malicious actions is beyond consideration.

Malicious Insider Demographics

Findings from a recent annual worldwide study on fraud may be instructive in terms of defining general risk demographics for other types of insider attacks. The data also may help gauge potential magnitudes of consequences based upon skill level and access, among other factors.

According to the *2012 Global Fraud Study* published by the Association of Certified Fraud Examiners, perpetrators of fraud with higher levels of authority and longer tenure within an organization tend to cause much larger losses than do managers and regular employees. In all but one region, between 77 and 86 percent of *reported* frauds were committed by employees and managers; however, owners and executives caused much higher monetary losses. According to the study, owners/executives caused losses approximately three times higher than managers, who caused losses approximately three times higher than did employees. The study attributes this to the fact that individuals with higher levels of authority generally have greater access to an organization's assets and mechanisms to override anti-fraud controls. For the same reasons, they generally are more capable of concealing their nefarious activities for a longer period of time before they are detected.

The study also notes that collusion by multiple individuals to commit fraud, especially when their combined efforts enable them to circumvent or disable anti-fraud controls, consistently result in more than double the losses than those involving lone insiders.

Source: Association of Certified Fraud Examiners, *2012 Global Fraud Study: Report to the Nations on Occupational Fraud and Abuse,* www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf, accessed July 3, 2012.

Medium- to High-Likelihood and High- to Catastrophic-Consequence Region

The medium- to high-likelihood and high- to catastrophic-consequences quadrant (the shaded area in Figure 4 below) contains the seven scenarios that were assessed to pose the highest risk from insider threat in terms of the likelihood of success and the severity of consequences should they be successful. More than half of these attacks are kinetic in nature, using IEDs. In all but one, the perpetrator is most likely to be a *low-skilled insider* who maintains the required access to facilities and areas where a kinetic attack could cause the greatest impact. By virtue of their frequency of contact with or knowledge of the target, the insider has a unique advantage over an outsider attempting to execute the same attack because he or she may know how to exploit specific temporal or physical weak spots in the system that maximize the likelihood of success.

The evolving nature of terrorist groups and the ease with which the materials for an IED can be inserted into critical infrastructure systems make this type of attack a high-risk scenario.

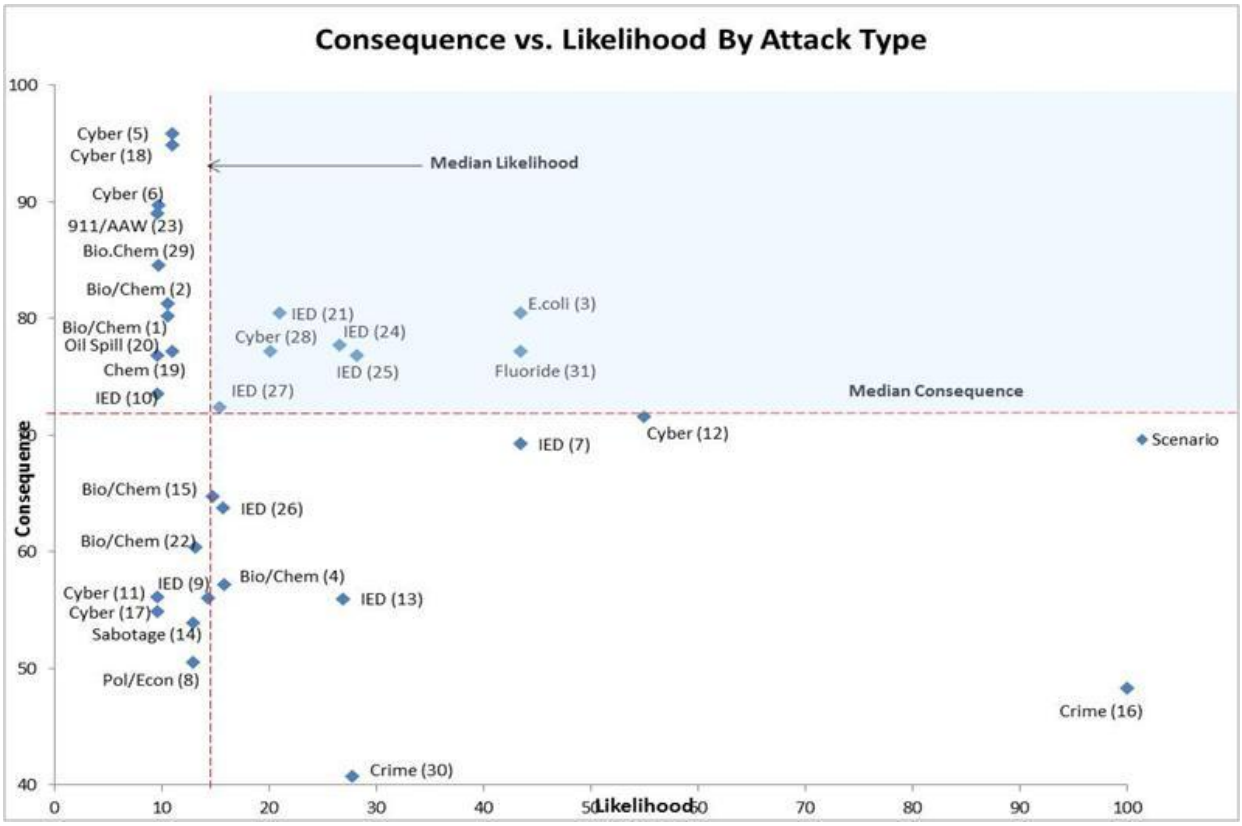

Figure 4. Medium- to High-Likelihood and High- to Catastrophic-Consequence Scenario Quadrant (shaded in blue)

In **Scenario 24**, the Transportation Sector (Aviation Subsector) is victimized by an insider who is an unwitting participant in illegal activity that he or she assumes to be non-kinetic in nature. In this scenario, a drug smuggling ring originally recruits a baggage handler at a major U.S. airport to place packages of illegal drugs in the cargo hold of passenger planes, presumably for personal monetary gain. Unbeknownst to the baggage handler, the drug smugglers are aligned with a terrorist group. Having convinced the insider to act on their behalf repeatedly in the drug running operation by shepherding illegal packages through layers of airport security, at some point the smugglers switch out the drugs with an IED that detonates while the aircraft is in flight. In this "social engineering"[41] scenario, the insider's willingness to disregard policies and procedures is exploited to the point where the insider becomes desensitized to the malicious nature of his original actions, having repeated them a sufficient number of times.

[41] At its core, "social engineering" is the art of exploiting trust, relationships, and human interactions and psychology to achieve a goal. Within the context of this NRE, a social engineering attack involves an insider using human interaction – social skills – to obtain or compromise information about an organization, to include its facilities, security posture, IT systems and networks, and data. If an insider cannot obtain enough information from one source, he or she may contact another source within the same organization to build upon or verify previously gathered information. This definition was adapted from U.S. CERT Security Tip (ST04-014), "Avoid Social Engineering and Phishing Attacks," available at http://www.us-cert/ncas/tips/st04-014, from CSO Online, available at http://www.csoonline.com/article/514063/social-engineering-the-basics#1.

- The immediate consequences of such an attack include loss of life, which varies based upon the number of passengers and crew onboard the commercial aircraft, as well as the population density at any potential impact site or debris field. This value could range from one dozen to several hundred individuals. The short- and long-term economic impacts of this scenario would be significant. According to a study by the International Air Transport Association (IATA) following the attacks of September 11, 2001, the aviation industry lost $13 billion in 2001 and a further $11.3 billion in 2002. The IATA report also cited a nominal gross domestic product decline of $142 billion over the 10-year period following the 9/11 attacks.[42]
- By virtue of their access to sensitive or secure areas of facilities, aviation employees pose a credible threat to commit or facilitate terrorist acts as insiders. Many have knowledge of aviation security procedures and ample opportunity to commit unlawful acts. Several well-documented cases involve aviation employees who have used their access privilege and knowledge to engage in criminal activity such as drug smuggling and theft. In addition, several cases involve terrorist organizations that either sought to recruit aviation employees to assist them in planning or conducting terrorist attacks or tried to gain employment as aviation workers for the same purposes. Recent examples include a June 2012 drug smuggling plot involving aviation employees (including TSA airport screeners and security officials at Los Angeles International Airport) and large-scale gun and cocaine smuggling operations in 2009 and June 2012 that involved dozens of foreign-based baggage handlers.[43,44]

Scenario 28 in the medium- to high-likelihood and high- to catastrophic-consequences quadrant is an exception to the kinetic attack trend mentioned above and was discussed in detail during DHS's espionage tabletop exercise.

- **Scenario 28** is essentially a "go-to-war" scenario that is part of a complex, long-term, multi-sector espionage and contingency attack plan designed to buy time for a foreign adversary to take military action while delaying a U.S. military response. At its core is a cyberattack on multiple rail control centers' Supervisory Control and Data Control (SCADA) scheduling system intended not to destroy the entire system but to scramble train schedules using an algorithm that disrupts the military logistics system for up to 10 days. Specifically, this scenario involves a foreign nation-state recruiting multiple insiders to conduct integrity attacks on railroad control centers using such vectors as SCADA and other automated scheduling and routing control systems.[45] In this plan, an

[42] International Air Transport Association, *The Impact of September 11 2001 on Aviation*, Switzerland: September 2011: 3, www.iata.org/pressroom/Documents/impact-9-11-aviation.pdf, accessed September 12, 2012.
[43] Los Angeles Times, "TSA drug smuggling case is 'significant' security breach, feds say," April 26, 2012, http://latimesblogs.latimes.com/lanow/2012/04/tsa-drug-smuggling-case-is-significant-security-breakdown-feds-say.html, accessed August 27, 2012.
[44] Aviationpros.com ,"Baggage Handlers Arrested For Smuggling Tons Of Cocaine," June 7, 2012, http://www.aviationpros.com/news/10726451/baggage-handlers-arrested-for-smuggling-tons-of-cocaine, accessed August 27, 2012.
[45] Time constraints of the NRE tabletop exercise dictated that the team had to focus on one critical infrastructure sector, in this case rail. Therefore, the team did not discuss associated attacks on airlift via the Federal Aviation Administration Network Operations Center, ports, and telecommunications that most likely would also be targets of this type of broad-based foreign espionage campaign.

outside programmer develops a malicious "sleeper" code that the insider(s) injects in the appropriate scheduling and switching control systems to be triggered at a later date. The insider(s) also installs cellular gateways or "back doors" at multiple SCADA locations as a back-up to the malicious code. This type of attack also could include corrupting, fooling, or manipulating associated radio frequency identification tags, readers and databases to make railcars "go missing" or be misidentified as another vector to increase the effects of attack.[46]

- While cyberattacks may not be considered classic high-to-catastrophic consequence events, this attack results in a potentially severe impact, in which a foreign country in collusion with well-placed malicious insiders causes the degradation or disruption of U.S. military movements.[47] The success of this plan depends upon recruiting the right mix of insiders within multiple organizations and sub-sectors that would have to be identified in a pre-operation target package. The implanted or recruited insiders would not require a great deal of expertise but only *time* and *access* to gather specific information. The focus of their long-term espionage effort is to identify and assess exploitable seams between the military and the outside world–from hardware to people. Potential targets include: SCADA/scheduling control systems, military storage locations, military equipment transport nodes and termini, and rail company logistics databases and management procedures. The subject matter experts participating in the tabletop exercises for this NRE generally agreed that this espionage plan was the most comprehensive and difficult to recognize of the four plans presented because it affects so many sectors over such a potentially long period of time. If unnoticed or ignored, small blips and infractions committed at the hands of trusted insiders could lead to an exponential increase in the threat and consequences over time. If this activity were executed methodically and within acceptable norms for error, the subject matter experts were concerned that most if not all of the activity might go unnoticed at the national level.

[46] Beginning in the 1990s, most North American Class I railroads were equipped with RFID readers and tags (transponders) as an automated, remote means to detect, identify, and track rail cars real-time via radio waves to a back-end server (database). According to one study, depending upon system configuration and stage of use, RFID systems are vulnerable to: attacks on authenticity, integrity, confidentiality, and availability; eavesdropping, man-in-the-middle attacks; denial of service; spoofing; and. power attacks. See Qinghan, Xiao, Thomas Gibbons and Harvé Lebrun, "RFID Technology, Security Vulnerabilities, and Countermeasures," in *Supply Chain: the Way to Flat Organization*, Julio Ponce and Adem Karhoca (Eds.), January 2009: 365, http://cdn.intechopen.com/pdfs/6177/InTech-Rfid_technology_security_vulnerabilities_and_countermeasures.pdf, accessed July 15, 2012.

[47] It is difficult to quantify losses from a cyberattack. A Congressional Research Service (CRS) report stated that in 2003 worldwide losses from worms and viruses was $13 billion while the impact of worldwide cyberattacks that year was $226 billion. More recently, the Ponemon Institute estimated that cyberattacks have an annualized median cost to organizations of $3.8 million per year. See Cashell, Brian, William D. Jackson, Mark Jickling, and Baird Webel, *The Economic Impact of Cyber-Attacks*, CRS Report for Congress RL32331, Washington, D.C.: The Congressional Research Service, Library of Congress, April 1, 2004: 1; and Ponemon Institute, *First Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies*, Traverse City, MI: Ponemon Institute LLC, July 2010: 2, www.nacha.org/userfiles/File/Internet_Council/Resources/Ponemon%20cost%20of%20cybercrime.pdf, accessed July 12, 2012.

Third-Party Insiders and SCADA

Vitek Boden was an engineer for a firm that installed remote-control and telemetry SCADA equipment for the sewerage pumping stations of the Maroochy Shire Council in Queensland, Australia. Denied employment with the Council before leaving the company on poor terms, he decided to get even with his former employer by attacking the control system he helped install. Using a stolen computer and radio equipment attached to a laptop, Boden drove around the area from February to April 2000 issuing radio commands that released more than 8000,000 liters of raw sewage into local parks, rivers, and hotel grounds.

Boden altered electronic data in the pumping stations to cause operational malfunctions, e.g., making pumps run when they should not, preventing alarms from reporting to the central computer, and disrupting communications between the central computer and the pumping stations. The laptop software was developed to change configurations in the pumping stations computers. Boden hoped to leverage his expertise to land a job with the Council to fix the problem he was causing. Never employed by the organization he attacked, Boden's knowledge made him the ultimate insider who was able to evade digital forensics for more than 2 months before coming under suspicion.

[a] Abrams, Marshal (The MITRE Corporation) and Joe Weiss (Applied Control Solutions), malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia, July 23, 2008.

Low-Likelihood and High- to Catastrophic-Consequence Quadrant

The ten malicious insider risk scenarios in the low-likelihood and high- to catastrophic-consequences quadrant (shaded in Figure 5 below) are significant because they represent a sampling of complex, targeted, "worst nightmare" attacks that pit the highly motivated and highly skilled insiders–often with foreign government, terrorist, or organized criminal collusion--against some of the Nation's most relatively robust and well-defended critical infrastructure sectors, facilities, and supporting assets in the post-9/11 operating environment. If successful, they could create potentially catastrophic, national-level consequences in terms of any combination of loss of life, business continuity, direct and indirect economic losses, and deleterious effects on the national psyche.

The two primary types of attacks that fall in this quadrant are: 1) specialized cyberattacks on financial systems, and 2) sophisticated chemical or biological attacks. Because of the level of sophistication and specialized access and skill required for all of these attacks, including the two kinetic scenarios, *high-skilled* insiders are the most likely perpetrators of these low likelihood and high-to-catastrophic consequence events.

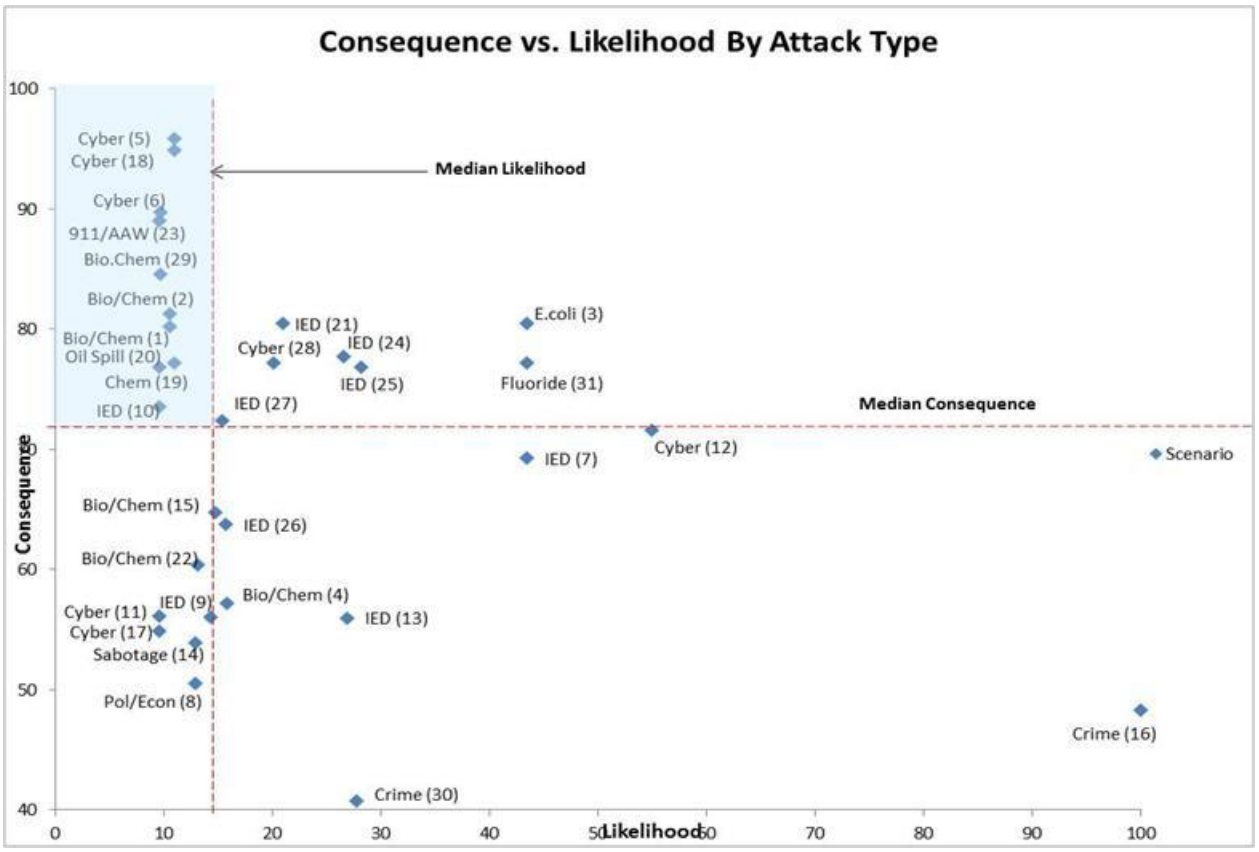

Figure 5. Low-Likelihood and High- to Catastrophic-Consequence Scenarios (shaded in blue)

Specialized Cyberattacks on Financial Systems

A single cyberattack generally is not considered catastrophic. Officials have confirmed that the collective result of ongoing cyberattacks may meet the threshold of a catastrophic attack but that there are very few single targets of national strategic importance that could suffer economic damage in the hundreds of billions of dollars range.[48] All three insider cyberattack scenarios in this quadrant target financial institutions or supporting critical assets that serve as clearing houses or messaging services for international trades and banking.

Highlighting the potential severity of these types of attacks is one scenario that received considerable attention during the Alternatives Futures Workshop and the Espionage Tabletop Exercise for this NRE. **Scenario 6** involves a cyberattack on a financial clearing house that manages security transactions. In this scenario, a nation-state-sponsored organized crime group with links to the regime coerces a clearing house employee, either on the software development or vulnerability management team, to attack that organization with the goal of creating capital flight from the United States markets. The insider would exploit that organization's dependence upon time by manipulating the integrity of the server that controls the time stamps on daily

[48] Cashell, Brian, William D. Jackson, Mark Jickling, and Baird Webel, *The Economic Impact of Cyber-Attacks*, CRS Report for Congress RL32331, Washington, D.C.: The Congressional Research Service, Library of Congress, April 1, 2004.

transactions via a "zero-day" exploit code that affects how trades are recorded. Given the paperless nature of today's financial trades, the attack would include tampering with the back-up systems to prevent rollbacks that attempt to undo the bad transactions. The insider would design the attack to last long enough to reap a cash-out worth millions of dollars before leaking the incident to the news media to maximize damage to the U.S. financial sector.

Highlighting potentially critical points of failure in the digitized financial sector, one study asserts that the technological dependency of securities exchanges upon IP-based platforms has dramatically increased the industry's exposure to reputation, market and operational risks. Further, the magnitude and speed by which fraud can be committed has increased with the convergence of once-private networks online.[49]

The subject matter experts supporting the tabletop exercises agreed that targeting critical financial control systems is extremely difficult to achieve remotely or wirelessly. As such, this attack would require a highly-skilled, stealthy, and motivated insider to place the codes on the clearing house computers. [50] The subject matter experts also considered this attack plan to be so complicated that it not only would require finding just the right insider to develop and emplace complex, malicious code in a highly structured change management environment, but also it would require multiple insiders working together.

The clearing house attack was assessed as a low likelihood event given that it targeted a regulated industry with tight hiring and cyber security controls. DHS is not aware of a nation-state with this level of sophistication trying to undertake this type of attack, especially with the use of an insider. The subject matter experts conceded that such a plan would be difficult to execute but not impossible, with several positing that if some entity or rogue state truly wanted to severely damage the U.S. economy regardless of the global implications, a successful attack of this type would accomplish their goals.[51] Making money is only a by-product of this attack scenario. Targeting a financial control system would have immediate effects with potentially long-term implications for the U.S. capital structure on which even rogue nation-states and criminal or terrorist organizations often depend.

The attack scenario, if successful, was assessed to have catastrophic consequences for the U.S. economy depending upon its timing, duration, and scope. One subject matter expert characterized the clearing house as the "heartbeat" of the financial industry in addition to being a vital commercial asset. Some posited that a cyberattack of this type and magnitude could cross a "red line" as an act of war (assuming such a tripwire exists).

---

[49] Kellermann, Tom and Valerie McNevin, *Capital Markets and E-fraud: Policy Note and Concept Paper for Future Study*, World Bank Policy Research Working Paper, May 2005: 1, http://elibrary.worldbank.org/content/workingpaper/10.1596/1813-9450-3586, accessed December 22, 2012. This paper also outlines seven E-fraud scenario case studies in which hackers did (and insider could) compromise systems for illegal purposes.

[50] Capital markets have command and control systems that can be exploited. Approximately 65 percent of financial trades are made using high-frequency machines that use code to control transactions.

[51] The findings of a 2009 National Cyber Defense Initiative *ad hoc* group workshop concluded that high-impact, large-scale attacks targeting the entire Banking and Finance Sector are "theoretically possible and under-analyzed." Furthermore, no available studies discuss the capabilities that transnational organized crime groups or nation states actually have to conduct such an attack or to provide the type of software exploit code required. Also lacking is an analysis of the risk and unintended consequences the crime groups or nation-state might incur in an attack on U.S. capital markets given the global nature of the Nation's economy and their reliance upon its stability.

- Extended delays or failure of clearing corporation operations would, at a minimum, inject unprecedented uncertainty into the markets and perhaps cause them to suspend operations temporarily. Similarly, a failure in the data processing or communications systems in a subsidiary could leave millions of transactions incomplete, halt investment activity in most U.S. securities for an uncertain period, and devastate investor confidence in the U.S. financial markets–and their ability to provide accurate prices or efficient matching of buyers and sellers–with possible worldwide spillover.[52]

Workshop discussions on this scenario yielded two key points regarding malicious insider threats that apply to all U.S. critical infrastructure sectors and mission-critical support assets.

- **Identifying Critical Assets within Critical Infrastructures.** The subject matter experts highlighted the need to identify systemically critical infrastructures and assets within critical infrastructures to ensure that they are hardened against becoming single points of failure. Hardening measures would include not only physical security measures but also fully integrated cybersecurity and human resource protocols to ensure that no high-risk behaviors or activities fall through the cracks. The subject matter experts overwhelmingly agreed that employees of designated critical infrastructures and assets should be held to a high standard that may include gradations of standards among positions of diverse levels of access, authority, and trust. In addition, private entities should have the appropriate mechanisms for requesting and receiving background and watch list information from the Federal Government on potentially high-risk prospective employees.
- **Back-Up Systems as Secondary Targets.** Malicious insiders and foreign adversaries could gain the advantage in creating catastrophic consequences by incorporating back-up command and control systems and software in their cyberattack plans to hinder response and recovery. In preparation for an attack, they may attempt to acquire the organization's contingency or continuity of operations plans, so that they know how to disrupt back up plans and systems. For example, one subject matter expert noted that a typical electric power transmission or pipeline system back-up site can be made operational in a reasonably short time frame to prevent serious consequences. In order for an attack to be successful, the malicious actors would need to delay or disrupt this backup capability.

Sophisticated Chemical or Biological Attacks

In contrast to the cyberattack scenarios in this quadrant, a single successful chemical or biological attack could cause catastrophic loss of life and severe, cascading economic and national security consequences. As stated in the *2010 National Security Strategy*, the gravest threat to the nation is a weapon of mass destruction in the hands of a terrorist.[53]

In these scenarios, the weapon of mass destruction is planted or dispersed by an insider able to circumvent protection systems regarding acquisition and transport of the material, which is generally a more difficult task for an outsider to achieve. Insiders are likely to have easier access

[52] Clancy, Mark G., "Cyber Threats to Capital Markets and Corporate Accounts," Congressional Testimony to the House Committee on Financial Services Subcommittee on Capital Markets and Government Sponsored Enterprises, June 1, 2012: 4, www.hsdl.org/?view&did=711622, accessed August 28, 2012.
[53] *2010 National Security Strategy*, Washington, D.C.: The White House, May 2010: 4. www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf, accessed August 3, 2012.

to specialized materials in the medical, industrial, and transportation arenas; the theft, sabotage, or weaponization of these materials does not have to create mass casualties or a meltdown to instill panic and fear.

Scenario 29 represents the low likelihood, non-nuclear weapon of mass destruction attack risks assessed for this NRE. The scenario involves an insider recruited by a terrorist group to facilitate a wide-area chemical or biological dispersal attack on a major U.S port.

- Although an outside adversary could conduct this type of attack, a well-placed and knowledgeable insider potentially shortens any reconnaissance and planning timelines and provides a vector for clearing existing physical security hurdles and exploiting target vulnerabilities to maximize the effects of an attack.

A successful wide-area biological or chemical attack on a major U.S. shipping port could produce catastrophic consequences. For the purposes of this scenario, analysts assumed that the port complex experiences a total disruption of port operations and intermodal connections. A chemical attack was assumed to kill or incapacitate the majority of the port's workforce and cripple the local industry. In addition, indefinite port closure would result in significant layoffs regionally and throughout the United States, and force the rerouting of millions of tons of cargo. The attack was also assumed to cause the indefinite closure of one of the United States' largest refineries, located near the port, significantly reducing national refining capacity. Significant uncertainties exist regarding the consequences of this scenario. For example, the impact of a wide-area biological or chemical attack depends on the type of agent deployed and its method of dispersal. If the agent allows for the port to be quickly brought back online, the impacts of such an attack would be minimized.

The Port of Houston

The port of Houston is the largest port in the state of Texas and a vital part of the City of Houston, the fourth largest in the United States with over 2.1 million people and an additional 3.85 million in the metro area.[a] The shipping business contributes to over 780,000 jobs in Texas, 1.5 million jobs throughout the United States, and generates $118 billion of economic activity in the state including over $3.7 billion in state and local taxes.[b] The Port of Houston plays a large part in the oil and gas industry and is home to a $15 billion petrochemical complex, the largest in the Nation.[c]

[a] City of Houston, *Houston Facts and Figures*, http:www.houstontx.gov/abouthouston/houstonfacts.html, accessed January 18, 2012.
[b] Reed, Michael, "Growth at Port of Houston Bodes Well for Job-Seekers," *Houston Regional News Bureau*, January 13, 2012. www.yourhoustonnews.com/news/favorable-trade-winds-ahead-growth-at-port-of-houston-bodes/article_b7863165-4409-51e2-a433-17e6e6b401f6.html, accessed January18, 2012.
[c] The Port Authority of Houston, *General Information: The Port of Houston, h*ttp:www.portofhouston.com/geninfo/overview2.html#portpast, accessed January 18, 2012.

Potentially Catastrophic Kinetic Events

One of the kinetic attacks in this quadrant is **Scenario 23** in which a disgruntled commercial airline pilot intentionally crashes a domestic passenger aircraft into a nationally critical asset. In this case, a *highly-skilled insider* decides to pursue a relatively simple mode of attack during the performance of his or her normal duties. Aside from commercial aircraft cockpit manning requirements, there are few countermeasures to prevent a deliberate, spontaneous, and potentially unrecoverable in-flight control maneuver by a pilot. As discussed in Scenario 23, the direct and indirect consequences of this type of attack could be catastrophic in terms of short-term and

long-term economic losses. The resemblance of this attack method to the attacks of September 11, 2001 could effect the American psyche in terms of willingness to fly, especially given that the pilot is "one of our own" this time.

EgyptAir Flight 990 Crash

The forced crash of a commercial aircraft by a pilot, while highly unlikely, is not unprecedented.

The National Transportation Safety Board (NTSB) determined that the crash of EgyptAir Flight 990 into the Atlantic Ocean 60 miles south of Nantucket, Massachusetts in October 1999 was caused by flight control inputs from the relief first officer that were initiated while he was alone on the flight deck. All 217 people onboard were killed. The NTSB investigation found no evidence of mechanical failure. The reason for the pilot's actions was not determined.

According to the NTSB's findings, the primary flight officer was unable to counteract the ongoing chain of negative control inputs upon his return to the cockpit.

Source: National Transportation Safety Board, *EgyptAir Flight 990, Boeing 767-366ER, SU-GAP, 60 Miles South of Nantucket, Massachusetts, October 31, 1999,* Aircraft Accident Brief, NTSB/AAB-02/01, March 13, 2002, www.ntsb.gov/doclib/reports/2002/AAB0201.pdf, accessed August 6, 2012.

Scenario 10 involves an attack by a recruited or self-radicalized insider who places an IED at a critical point in a dam facility to create a complete failure of the dam structure. In terms of difficulty, a comparison can be made to the intentional breech of the levees in Missouri during the 2011 flood. The U.S. Army Corps of Engineers had access to the technical specifications of the levee and were able to place the charges directly where they calculated the explosives would do the most damage and ultimately cause complete failure of the dam. The operation was costly, however, and the explosives were not initially effective in creating a significant breach.[54] This type of malicious insider operation, therefore, would be highly complex and difficult to execute effectively even when an insider acts on privileged information, for example, knowing weak spots in the dam structure by virtue of position, expertise, or access to technical specifications.

Low- to High-Likelihood and Medium-High- to High-Consequence Scenarios

The attack scenarios in the low- to high- likelihood and medium-high- to high- consequence region (Figure 6) tend to fall into the corruption and exploitation categories or represent versions of more serious attacks that involve insiders who must overcome screening hurdles before committing their malicious attacks. Some of the scenarios involve cybercrime. As with the high likelihood and high-to-catastrophic consequence scenarios, many of these attacks could be carried out by non-insiders but with much greater difficulty in terms of access.
The 14 attack scenarios in these two quadrants are highly diverse in type and target. The *exploitation attacks* identified are of particular interest since they are assessed to be occurring now at some level with the potential to create catastrophic consequences should the attack permeate an entire critical infrastructure sector or sectors. The high-likelihood and less-high-consequence cyberattacks have different characteristics from previously considered high-consequence cyberattacks, in that there is uncertainty as to whether an insider would be required

[54] Miller, Melissa, "Flood of 2011 Anniversary: Corps Maintains Birds Point Levee Breech Saved Billions in Damages," *Southeast Missourian,* April 25, 2012, www.semissourian.com/story/1841366.html, accessed August 8, 2012.

to inject viruses or create backdoors in software programs. An insider of any skill level could support this attack. The *kinetic attacks* represented in this quadrant are primarily IED attacks against targets with lower value or with more effective countermeasures in place than previously discussed IED targets.

- While this NRE maintains a national-level scope, some small but cumulative, non-coordinated attacks can have national-level economic impacts. For example, near-daily breaches of protected health care information could result in enormous amounts of health care fraud and identity theft.

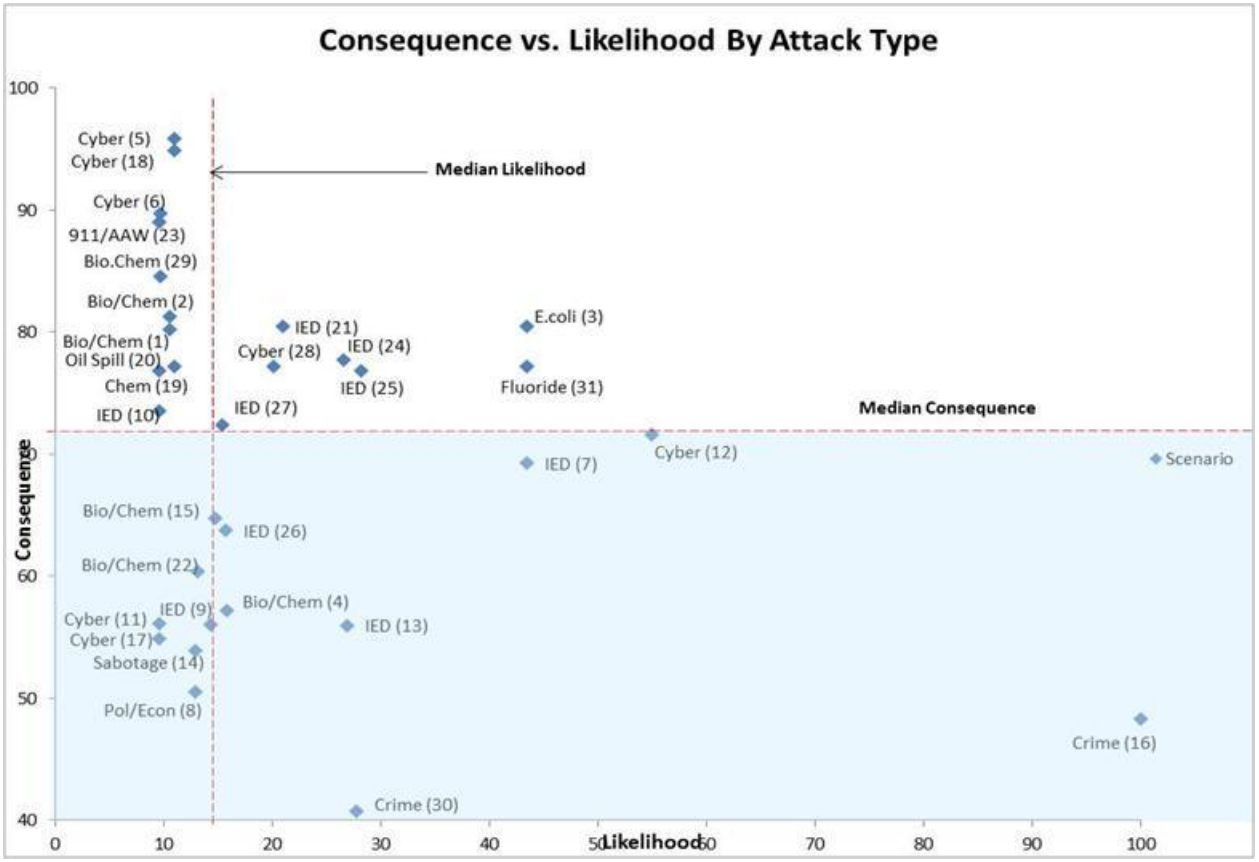

Figure 6. Low- to High-Likelihood and Medium-High- to High-Consequence Scenarios (Shaded in blue)

Exploitation Attacks

Exploitation attacks, such as **Scenario 16** (Medicare-Medicaid Fraud by Organized Crime) and **Scenario 30** (U.S. Border Corruption), are unique because the perpetrators want to maintain at least the appearance of normal operations for the targeted critical infrastructure under attack to maximize their personal or financial gain. These attacks can involve specific or systemic corruption throughout a particular infrastructure. At some point, these attacks reach a tipping point at which the exploitation can cause significant financial or psychological damage and severely erode public confidence in the system.

In **Scenario 16**, a foreign-based organized crime organization uses insiders to facilitate its Medicare and Medicaid fraud activities in metropolitan centers in at least 20 States. This multi-national criminal organization employs traditional approaches including creating service providers and sham storefronts, submitting high levels of fraudulent claims with stolen beneficiary information for non-existent services and equipment, collecting and laundering money, and disbanding the service provider before its illicit activities are detected. In light of potential changes to the current "pay and chase" process for public health care systems, the multi-national criminal organization would like to find new vulnerabilities in the claims system that might be harder for law enforcement to detect such as weaknesses in the program integrity and oversight process or a cyber weakness in the automated claims and payment processes. The multinational criminal organization has targeted administrative, database, and IT-skilled insiders in several major regional hospitals, regional Medicare Administrative Contractors, and Centers for Medicare and Medicaid Services who are involved with the claims and payment systems.

- Health care fraud is a large and pervasive problem that creates a costly drain on the U.S. health care system. Increasing the severity of this type of "slow-burn" criminal activity over the past decade or so has been the growing involvement of transnational and domestic organized crime groups who view health care fraud as a relatively low-risk, high-return, money-making scheme compared to drug trafficking and other dangerous pursuits.[55]
- In 2011 testimony to Congress, the Deputy Inspector General for the U.S. Department of Health and Human Services (HHS) highlighted the rising trend of violent and brazen new criminal enterprises in health care, stating that Medicare increasingly is being infiltrated by sophisticated, organized criminal networks and violent criminals. These criminals are acutely aware of the historic 90-day window of opportunity they have before Medicare program integrity contractors discover problems and report them.[56] A 2011 GAO report characterized as *critical* the need for better oversight of contractors providing services to Medicare beneficiaries to address fraud, waste, and abuse, and to prevent improper payments.[57]
- According to testimony of the Inspector General of HHS in 2011, "Medicare and Medicaid fraud, waste, and abuse cost taxpayers billions of dollars each year and put beneficiaries' health and welfare at risk."[58] Total national health care expenditures

[55] Business Wire, "LexisNexis identifies Top Trends in Health Care fraud, Waste and Abuse," February 16, 2012, http://www.businesswire.com/news/home/20120216006254/en/LexisNexis-Identifies-Top-Trends-Health-Care-Fraud, accessed March 8, 2012.

[56] Office of the Inspector General, U.S. Department of Health & Human Services, "A Perspective on Fraud, Waste and Abuse Within the Medicare and Medicaid Programs," Testimony of Gerald T. Roy, Deputy Inspector General for Investigations, before the U.S. House of Representatives Committee on Oversight & Government Reform, Subcommittee on Health Care, District of Columbia, Census and National Archives, April 5, 2011, http://oig.hhs.gov/testimony/docs/2011/Roy_Testimony_04052011.pdf, accessed March 9, 2012.

[57] King, Kathleen M. and Kay L. Daly, *Medicare and Medicaid Fraud, Waste and Abuse: Effective Implementation of Recent Laws and Agency Actions Could Help Reduce Improper Payments,* GAO-11-409T 9, Washington, D.C.: U.S. Government Accountability Office, March 2011: 17−18, www.gao.gov/products/GAO-11-409T, accessed August 13, 2012.

[58] Inspector General, U.S. Department of Health and Human Services, "Testimony of Daniel R. Levinson, Inspector General, U.S. Department of Health and Human Services to The United States Senate Committee on

reached $2.6 trillion in fiscal year 2010, according to data available from the Centers for Medicare and Medicaid Services. Medicare and Medicaid spending comprise approximately 35 percent of this total.[59] The FBI estimates that between 3 and 10 percent of this spending, on both public and private programs, is lost to health care fraud each year.[60] This translates into potential losses across the entire health care system ranging from $78 billion to $260 billion in FY 2010.[61]

In **Scenario 30,** a large, violent, and financially-motivated drug cartel recruits insiders and uses their access to U.S. border security infrastructure to facilitate the movement of drugs and money across the southern border. Over the course of three to four years, the insiders facilitate shipments of drugs and contraband into the United States. A large part of the plan's ultimate success hinges upon the cartel's ability to establish trust with border officials and law enforcement by feeding them information on the rival cartel. The net result is increased influence and cash flow for the cartel and eventual expansion of their territory while the U.S. government targets and slowly depletes the resources of the rival gang. Rather than instructing the insiders to stop legitimate cross-border commercial traffic, the cartel instructs them to use their access to help funnel illegal shipments through legitimate channels. In addition, the insiders would try to influence border policy by concentrating U.S. Government resources disproportionately on a rival cartel. The net effect is a nearly imperceptible increased flow of illegal shipments and a small but distinct shift in policy. Eventually, the cartel uses their significant cadre of insiders to manipulate the border infrastructure for their own purposes.

Finance," March 2, 2011, https://oig.hhs.gov/testimony/docs/2011/levinson_testimony_03022011.pdf, accessed June 24, 2012.

[59] Centers for Medicare and Medicaid Services, *National Health Expenditures 2010 Highlights,* www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/index.html?redirect=/NationalHealthExpendData/, accessed June 23, 2012.

[60] Federal Bureau of Investigation, *Financial Crimes Report to the Public, Fiscal Years 2010-2011*, Washington, D.C.: U.S. Department of Justice, 2011: 16, www.hsdl.org/?view&did=701476, accessed June 25, 2012.

[61] SAS Institute, Inc., *Combating Health Care Fraud: State-of-the-art methods for detection and prevention of fraud, waste and abuse in the health care industry*, 2010: 3, www.ucl.ac.uk/secret/events/event-tabbed-box/seminars-accordian/healthcare-fraud, accessed July 7, 2012.

U.S. Border Corruption

In testimony before Congress in 2010, the Assistant Director of the FBI's Criminal Investigative Division reported that the Bureau had 700 agents investigating corruption, 120 of them working on the Southwest border.[a] He highlighted information sharing efforts between the Bureau's Southwest Border Corruption Task Forces, local law enforcement intelligence centers, and Mexican legal attaches. He also noted the existence of corruption at other points of entry including ports and the Canadian land border.

In his 2011 testimony before Congress, the Commissioner of the Customs and Border Protection (CBP) noted that the CBP had doubled the size of its staff between 2004 and 2010 and that the pace of hiring had led to an increase in corruption investigations. He stated that 127 employees were arrested or indicted for corruption between 2004 and 2011 with 95 of the charges characterized as "mission compromising" or involving activity that violated the very laws CBP is supposed to enforce.[b]

The most notable case involving corrupt U.S. border officials strongly resembles the tabletop exercise scenario. In 2009, a CBP technician was convicted and sentenced to 20 years in prison for helping to import over 100 kilograms of marijuana, human trafficking, and bribery of public officials. The case sparked changes such as the Anti-Border Corruption Act of 2010, which required the CBP to institute polygraph tests for every law enforcement applicant by January 2013 and conduct periodic reinvestigations of all CBP personnel.[c]

[a] Federal Bureau of Investigation, "Testimony of Kevin L. Perkins, Assistant Director Criminal Investigative Division, Federal Bureau of Investigation, U.S. Department of Justice," March 11, 2010, www.hsdl.org/?view&did=14472, accessed June 29, 2012.
[b] "Statement of Alan Bersin, Commissioner, Customs and Border Protection on 'Border Corruption: Assessing Customs and Border Protection and The Department of Homeland Security Inspector General's Office Collaboration in the Fight to Prevent Corruption," June 9, 2011, www.dhs.gov/ynews/testimony/testimony_1307549850535.shtm, accessed June 29, 2012.
[c] Connolly, Ceci, "Woman's Links to Mexican Drug Cartel a Saga of Corruption on U.S. Side of Border," *The Washington Post*, September 12, 2010, www.washingtonpost.com/wp-dyn/content/article/2010/09/11/AR2010091105687.html, accessed June 29, 2012.

Cyberattacks

Cyber-attack scenarios in the low- to high- likelihood and medium-high to high-consequence quadrants (Figure 6) are primarily espionage-based and involve an insider capturing information on a critical U.S. asset or injecting a malicious code into the system. Each of these operations could be conducted remotely via a "digital insider," and there are accounts of foreign nations selling counterfeit hardware and software to the United States increasing the likelihood of backdoor vulnerabilities and latent viruses that seemingly would eliminate the need for an insider.[62] In cases where a nation-state uses a closely associated business in the United States to conduct the attack, an insider will add no unique value and is not needed. For other entities, there is significant opportunity for a low-skilled insider to inject malicious code created by another or for a high-skilled insider to create backdoor vulnerabilities in a software program.

[62] Between 2009 and 2010, a Senate Armed Services Committee investigation found 1,800 cases of counterfeit electronic parts in the DoD supply chain. The investigation identified a total of more than one million individual parts. See The Committee on Armed Services United States Senate, *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain*, Washington, D.C.: U.S. Government Printing Office, May 21, 2012: i, www.armed-services.senate.gov/Publications/Counterfeit%20Electronic%20Parts.pdf, accessed June 25, 2012.

Kinetic Attacks

The kinetic attack scenarios in the low- to high- and medium-high- to high-consequence regions (Figure 6) are all conducted using IEDs; however, the consequences in these cases are lower because the attackers target sectors that have countermeasures intended to reduce the impact of an explosive device, or because the potential target has less significance and fewer cascading effects than those of other potential targets.

Global Supply Chain Targeted Attacks.

Scenarios 8, **9**, **14**, and **15** in the low- to high-likelihood and medium-high- to high- consequence region (shaded in Figure 6) focus on disrupting the global supply chain. They are unique because the disruptions can occur at any point in the supply chain, which includes overseas facilities and non-U.S.-based contractors or organizations. Although previously raw materials, components, and finished products were manufactured and distributed primarily domestically, since the 1980s, U.S. firms have increasingly relied on foreign sources for commodities and products.[63,64] This trend has created a geographically-diversified set of suppliers, as well as involving more brokers, customs regulations, security requirements, and legislative actions related to importing/global sourcing, geopolitical issues, transfer points, and port issues. All of these factors contribute to a lack of visibility of the entire system/supply chain and increased vulnerability to terrorism, disruption stemming from geopolitical conflicts, and the potential for malicious supply chain penetration for espionage purposes and product tampering.[65]

Scenario 15 is an exploitation attack in which an insider contaminates materials used in pharmaceutical production. It occurs at the production location of many of the top pharmaceutical products sold in the United States. According to the IMS Institute for Healthcare Informatics, the top 20 selling prescription drugs in the United States were worth $78.5 billion dollars in 2010.[66] The loss of production and manufacturing facilities for an extended period of time could cause significant economic harm to the U.S. pharmaceutical market.

Another aspect of malicious insider supply chain attacks against pharmaceuticals raised during the NRE espionage tabletop discussions was the concern that an insider with foreign collusion could attempt to put a high-profile pharmaceutical company out of business by tampering with the manufacturing system that monitors drug quality control. As a result, the consumer public could lose confidence in the safety and integrity of the U.S. product while the foreign adversary or competitor gains a strategic market advantage.

---

[63] Marsh Consulting, *The Changing Face of Risk Management,* January 28, 2010: 16, www.rimas.org.sg/files/The%20Changing%20Face%20of%20Risk%20Management.pdf, accessed September 5, 2012.

[64] Agrell, J., Lindroth, Robert, and Norman, Andreas "Risk, Information, and Incentives in Telecom Supply Chains," *International Journal of Production Economics* (Vol. 90, Issue 1), July 8, 2004: 4, www.uc3m.es/portal/page/portal/dpto_economia_empresa/home/seminars/Previous_years/Seminars_2008-2009/agrell.pdf, accessed May 18, 2012.

[65] U.S. Department of Homeland Security, *Strategy to Enhance International Supply Chain Security*, July 2007, www.dhs.gov/xlibrary/assets/plcy-internationalsupplychainsecuritystrategy.pdf, accessed August 31, 2012.

[66] IMS National Sales Perspectives™, "Top U.S. Pharmaceutical Products by Spending," April 7, 2011, www.imshealth.com/deployedfiles/ims/Global/Content/Corporate/Press%20Room/Top-line%20Market%20Data/2010%20Top-line%20Market%20Data/2010_Top_Products_by_Sales.pdf, accessed August 24, 2012.

Chapter 4: Exploring Alternative Futures for the Insider Threat to U.S. Critical Infrastructure

To support the development of this NRE, DHS hosted a workshop to elicit judgment from government and private industry subject matter experts on four alternative futures that could present challenges and opportunities related to malicious insider threats to U.S. critical infrastructure over the next 20 years. The alternative futures discussed are not intended to predict the future. Rather, they illustrate plausible combinations of uncertainties and contributing factors, based upon current analysis of insider threat trends, and they tell a series of compelling stories about how the nature and mitigation of insider threats could evolve if each future became a reality. These futures also provide perspectives that may help to guide and inform future policy and funding decisions. The workshop participants discussed potential signposts and indicators that might correspond to each alternative future, as well as strategic surprises that could bring chaos and significantly alter their trajectories. [67] The NRE alternative futures were developed with a methodology that considered a range of uncertainties for insider threat over a 20-year period from 2012 to 2032. The methodology is based on the 2008 U.S. National Intelligence Council *Disruptive Civil Technologies* report.[68] Appendix D provides a full description of the methodology used to develop the alternative futures. Appendix I contains a list of the workshop participants.

Analytic Assumptions

The Alternative Futures workshop participants based their analysis on the following assumptions, each of which is intended to be viable for the next 20 years:

- Insider threats to U.S. critical infrastructure will continue.
- Malicious insiders will be more technologically savvy and increasingly capable of defeating security countermeasures that are static, improperly scoped, or unable to keep pace with the evolving threat.
- The line between internal and external threats will be increasingly blurred because of the proliferation of digital, Web-based technology within business and control systems.
- Major investments in U.S. critical infrastructure to mitigate insider threats will not be universal or consistent.
- Innovation and/or effective risk management will be able to mitigate certain aspects of insider threat risk.

[67] A strategic surprise is an unanticipated incident or event that causes significant disruption or damage to a critical infrastructure and/or supply chain. See the U.S. National Intelligence Council, *Disruptive Civil Technologies*, Conference Report CR 2008-07, April 2008: v, www.dni.gov/nic/confreports_disruptive_tech.html, accessed August 20, 2012.

[68] U.S. National Intelligence Council, *Disruptive Civil Technologies: Six Technologies with Potential Impacts on U.S. Interests Out to 2025*, Conference Report CR 2008-07, April 2008, www.fas.org/irp/nic/disruptive.pdf, accessed August 20, 2012.

Key Themes

The workshop discussion yielded the following key themes regarding potential future landscapes for the insider threat to U.S. critical infrastructure over the next 20 years:

- Traditional, "low-tech" malicious insider techniques continue to remain viable, even in a technologically advanced future, because adversaries will continue to exploit targets that are easiest to access in the prevailing security environment.
- Migration to dependence on the "cloud" environment provides insiders significantly increased opportunities to execute systemic and repeatable attacks which could affect all critical infrastructure sectors and exploit their virtual supply chain vulnerabilities, particularly with regard to the feasibility of both hypervisor and inter-virtual machine (VM) attacks by employees and third-party software vendors.[69]
- The trend toward blended (cyber and physical) attacks against critical infrastructure will force the issue of a convergence between cybersecurity and physical security to foster a more holistic approach to managing risk against a much more sophisticated and broad spectrum insider threat.
- Globalization and outsourcing as they relate to U.S. critical infrastructure will increase current challenges associated with employee privacy and trust issues in any alternative future environment.

Insider Threat Uncertainties over the Next 20 Years

The workshop participants ultimately selected **governance** and **insider capabilities** as the two major uncertainties that will drive the alternative futures related to the insider risk to all 16 U.S. critical infrastructure sectors.[70] Figure 7 outlines the four alternative futures identified in this NRE that are based upon the pairings of these two uncertainties and their associated factors, which describe possible boundaries for the general state of each uncertainty.

[69] The hypervisor, also called a virtual machine (VM) manager, serves as the control panel ("brain") of the virtualized "cloud" infrastructure, allowing multiple operating systems (OS) to share a single hardware host. The hypervisor is a layer of abstraction between VMs and the underlying hardware, allowing for the dynamic allocation of system resources. Although each OS appears to have the host's processor, memory, and other resources all to itself, the hypervisor actually controls the host processor and resources, allocating what is necessary to each OS and ensuring that the VMs do not disrupt one another. If the hypervisor is compromised, then the entire infrastructure can be controlled and infected at once. Inter-VM attacks involve individual virtual machines attacking other virtual machines. This is problematic because most cybersecurity technologies have no visibility into what occurs within virtual machines. See *Changing the Game for Anti-Virus in the Virtual Datacenter*, Trend Micro White Paper, September 2012: 2, and http://searchvirtualization.techtarget.com/definition/virtual-machine. For further discussion on hypervisors and VMs, see also Mitchell, Robert L., "Hypervisor as virtualization's enforcer?," August 10, 2010, http://www.computerworld.com/s/article/9179910/Hypervisor_as_virtualization_s_enforcer_

[70] Within the context of the NRE, uncertainties represent areas that will be of significant importance in shaping the trajectory of the insider threat to U.S. critical infrastructure over the next 20 years. The uncertainties discussed here are by no means the only two that potentially could affect the future of the insider threat; however, these are the two which the workshop participants assessed to be the most impactful and compelling based upon current trends, available insider threat data, and published research.

		Insider Capabilities	
		Traditional Techniques	**Technology Enhances**
Governance	**Haphazard**	**Tried and True Will Do**	**Mission Impossible**
	Effective	**Advantage Good Guys**	**Cold War**

Figure 7. Insider Threat Alternative Futures Matrix

Governance

For the purposes of this NRE, the subject matter experts adopted a performance-based risk management approach to governance, relating to creating an organizational framework to counter the evolving insider threat that includes the following:

- Clearly defined insider threat program policies and procedures;
- Expectations for consistent training, compliance, and policy enforcement that are scalable across organizations and critical infrastructure sectors;
- Appropriate parameters for employee screening and behavioral monitoring that take into account legal and privacy considerations, as well as potentially negative impacts on operations, productivity, and morale;
- Robust cooperation and coordination between those responsible for the cyber and physical security aspects of the insider security program; and
- Safety and soundness through governance, in which the end goal is to protect critical infrastructure assets and insulate them from risk.

The workshop participants unanimously agreed that risk management is a function of good governance. After establishing a sound governing structure for risk management, leadership must determine how best to execute the created responsibilities. The subject matter experts described the lack of an overarching industrial policy standard regarding insider threats to critical infrastructure as one of our Nation's greatest weaknesses. While regulations exist in certain sectors and industries, others devote little attention and few resources to insider threats. Even where insider threat policies and programs are in place, execution, enforcement, and verification may be inconsistent at best. In addition, some of these policies and programs may not address the many nuances of the evolving insider threat that cross personnel, physical, and cybersecurity domains. Several subject matter experts voiced concern that, in the future, effective policies *must* address a stakeholder's ability to identify, monitor, and deal with at-risk employees without eroding morale and productivity.

Generating effective, reasonable, and actionable policies to govern an organization requires an environment of employee trust. As a counterpoint to this, the workshop participants thought that the ability to effectively monitor a diverse set of insider threats and detect early indicators of

potential insider activity will depend heavily upon changes to U.S. policy and laws regarding employee privacy, particularly in the private sector.

A recurring theme throughout the "effective" versus "haphazard" governance discussion was a concern about the traditionally bifurcated cyber and physical security worlds. Workshop participants agreed that governance should integrate both aspects of security to protect critical assets against insider threats. The workshop participants posed the following questions: Does the Chief Information Security Officer (CISO) or the Chief Security Officer (CSO) implement policies to preserve the integrity of access controls; i.e., who is more technical? At what point does organizational governance change to deal with the responsibilities of the CSO and CISO? The subject matter experts had no specific answers to these questions, but did agree on the need for CISO-CSO collaboration, supported by appropriate changes in governance and sufficient funding to make the collaboration effective. WikiLeaks and similar cases were cited as reasons that policy alone–just like improved technology–is insufficient to deal with the full range of insider threats.

Insider Capabilities

Based upon several of the key assumptions that address current threat data and trends, the workshop participants agreed that juxtaposing malicious insider capabilities with varying states of governance affecting insider risk management provided the most compelling range of alternative future scenarios. Within the context of this NRE, capabilities refer to the diverse and evolving suite of tactics, techniques, and procedures available to the malicious insider, who continually is forced to make trade-offs in terms of how and when they can be effectively used against the existing security environment. These capabilities are expected to span the full range from relatively "low-tech" kinetic and cyberattacks to generally sophisticated, targeted, and technologically advanced techniques. Their selection and successful employment will involve a dynamic series of trade-offs depending upon the nature of the prevailing governance environment. In a worst-case scenario, the malicious insider – through responsibilities gained by advancing within the organizational chain – may have a major role in building the existing risk management culture. This is a force multiplier when combined with cyber vulnerabilities that the insider has either designed or systematically ignored. Of particular interest to the group was the premise that most insider threats today are facilitated by cyber vulnerabilities and that the problem only becomes worse as trust in the "cloud" increases. The "cloud" currently is not considered critical infrastructure for the purposes of risk management.

The Advantage Good Guys and Mission Impossible futures present the most compelling challenges for U.S. critical infrastructure stakeholders within the context of the juxtaposed uncertainties and factors and are highlighted below. Appendix G provides more detailed descriptions of all four alternatives futures discussed during DHS's workshop and depicted in Figure 7.

Alternative Future: Advantage Good Guys

To succeed in the Advantage Good Guys alternative future, the traditional insider must work harder and risk exposure to identify and target what is *not* guarded in his or her domain. Effective governance (as it applies to U.S.-based versus overseas operations) creates a higher probability of detection, greatly reducing the risk of an insider attack. In this world, insider collusion may become more of an imperative to overcome layered defenses with more physical

and cyber threat mitigation controls in place. Even collusion may not be enough to defeat more robust insider threat detection programs that incorporate advanced and potentially automated behavioral analysis tools.

Workshop participants stated that a higher risk of exposure and detection, as well as the relative localization of the threat, make successful insider attacks less likely. Effective and integrated physical and cybersecurity policies will make it more difficult for insiders to act alone.

In addition, both public and private organizations will need to assess the best security procedures that also respect employee privacy, a trade-off that will test effective governance in the face of advances in the digital world. To be highly effective, insider threat programs must incorporate both behavioral-analysis tools and technical solutions, at least some of which may be automated. Insiders in the Advantage Good Guys world may be forced to resort to more traditional tradecraft and capabilities, at least in the short term, to circumvent effective countermeasures. The workshop participants envisioned that the Advantage Good Guys and Cold War alternative futures may go back and forth as each side strives to gain the advantage. In both worlds, more insider activity may be detected and prevented, but the "arms race" for technological measures and countermeasures continues.

Challenges

The identified challenges facing public and private critical infrastructure stakeholders in the Advantage Good Guys alternative future included:

Avoiding complacency by maintaining and continually evaluating effective governance in the face of constantly evolving threats;

- Striking a balance between operational efficiency/mission accomplishment and implementing comprehensive insider threat security programs that may be too severe and invasive;
- Managing and distilling enormous amounts of data from multiple sources, e.g., social media, physical detection systems, cyber, behavioral profiles, into actionable information.
- Maintaining situational awareness regarding "consumerization" of "high-tech" tools (e.g., logic bombs and rootkits) available on the open market and the Web;
- Recognizing that globalization of the workforce requires balancing exploiting new business opportunities against keeping plans and strategies secure; ;
- Maintaining employee trust in an increasingly globalized and "plugged in" world; and
- Retaining adequate funding for governance.

From this list of challenges, two major themes emerged as perpetual threats to effective governance with regard to U.S. critical infrastructure in any future scenario: *maintaining trust and loyalty in the new generation workforce* and the human and technical aspects of *globalization*.

Maintaining Trust and Loyalty in the New Generation Workforce

As the generation born between 1978 and 1994 becomes the dominant demographic in the global workforce, organizations will increasingly need to balance employee expectations of privacy and autonomy on the Internet against operational productivity and security. This generation expects

to be more connected to the Internet and to social networks, both of which could pose security risks to their employers. At the same time, any program designed to use social media postings as an indicator of insider threat will face numerous legal, policy, and technical issues. In addition, an overly-oppressive monitoring program could erode employee loyalty and interfere with productivity.

The subject matter experts echoed findings in current literature that the generation gap and changes in the culture, demography, and values of the future workforce will play a major role in any future insider risk mitigation environment that attempts to grapple with the complex and intertwining issues of workplace loyalty and corporate security. For example:

- According to an April 2011 BPW Foundation study, Generation Y/Millennials (born between 1978 and 1994) will comprise approximately 75 percent of the global workforce by 2025.[71]
- A 2008 Deloitte study describes Generation Y, which has been raised on the Internet, as tech savvy and socially-networked. Its members have an expectation of constant and immediate connectivity, as well as a "natural propensity to share information" through social media, even if it is unrelated to work responsibilities, which presents many new security challenges as the secure workplace becomes more networked and dispersed. The study asserts that these expectations could introduce a new type of risk in a secure work environment.[72]
- The 2011 *Cisco Connected World Report* found that approximately 56 percent of college students and young professionals worldwide (or 66 percent of U.S. respondents) indicated that if they encountered a company that banned access to social media, they would either decline the job offer or accept it and find a way to work around such policies. Twenty-nine percent of the college students and 30 percent of the end users responded that it would be their right, not a privilege, to work remotely with a flexible schedule. The study is based upon the responses of more than 2,800 individuals in 14 countries.[73]

According to the Office of the National Counterintelligence Executive, the cultural shift in which the U.S. workforce increasingly places greater value on access to information and less emphasis on privacy or data protection may increase productivity, but at a higher risk to information and system security.[74] The ongoing challenge for mitigating the insider threat to U.S. critical infrastructure is how to implement prevention policies and procedures. These policies and

[71] BPW Foundation, "Snapshot of Generation Y," April 2011. Cited in Dhawan, Erica, "Gen-Y Workforce and Workplace Are Out Of Sync," *Forbes*, January 23, 2012, www.forbes.com/sites/85broads/2012/01/23/gen-y-workforce-and-workplace-are-out-of-sync/, accessed September 11, 2012.
[72] Gelles, Michael, David Brant, and Brain Geffert, *Building a Secure Workforce*, Deloitte Consulting LLP, 2008: 5, www.deloitte.com/view/en_US/us/Industries/US-federal-government/764ef33b4010e110VgnVCM100000ba42f00aRCRD.htm, accessed April 25, 2012.
[73] Cisco, *2011 Cisco Connected World Report*, www.cisco.com/en/US/solutions/ns341/ns525/ns537/ns705/ns1120/2011-CCWTR-Chapter-3-All-Finding.pdf, accessed 11 September 11, 2011.
[74] Office of the National Counterintelligence Executive (ONCIX), *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collections and Industrial Espionage, 2009-2011*, Washington, D.C., October 2011:7.

procedures must balance defending increasingly fluid organizational boundaries and maintaining a corporate culture of trust among a new workforce generation with high expectations of privilege and access.

The public and private sector will also need to effectively manage a myriad of social media, physical, cyber, and behavioral data as they relate to insider threat. As one report on information security explains, the insider threat is so complex that it will require multiple layers of security, including initial and ongoing vetting, continuous education, and maintaining a strong and enforced security policy that addresses social networking used by staff.[75] According to a recent survey by Gartner, currently less than 10 percent of corporations have a security monitoring plan in place for social media use; however, by 2015 approximately 60 percent of the corporations responded that they *plan* to implement a formal security monitoring plan for employee use of social media.[76]

Globalization

Globalization will continue to complicate the analysis and mitigation of insider threats. The subject matter experts repeatedly mentioned two aspects of increasing globalization that affect the future security of U.S. critical infrastructure, particularly in the private sector: 1) divided loyalties, and 2) an increasingly-networked global business environment. Both have cumulative effects on the opportunities, access, and motivations potential malicious insiders will have to conduct attacks. In a world that becomes progressively smaller by virtue of increased and nearly instantaneous connectivity, the opportunities for risk from malicious inside actors become exponentially greater. The subject matter experts posited that some of the worst scenarios in terms of testing U.S. response and resolve against diplomatic sensitivities would involve members of an expatriate community who exploit their access to industrial or network control systems to harm U.S. critical infrastructure.

Divided Loyalties. In addition to future challenges surrounding diminishing workforce loyalty and insider threats, the subject matter experts expanded their discussion beyond generational factors to global concerns. Specifically, they expressed concern as to whether owners and operators are prepared to identify and deal with members of an increasingly multicultural workforce whose emotional, familial, or business ties to their countries of origin or to a more global community could override loyalty to their employer and/or their allegiance to the United States.

A guide to promoting a secure workforce produced by the consulting firm Deloitte suggests that employees who are naturalized citizens may be exposed to a unique set of pressures through their connections to their country of origin and culture that leave them more vulnerable to exploitation by nation states, transnational organized crime groups, drug cartels, and terrorists. Deloitte's report points out that even employees with no malevolent intent may be susceptible to

[75] Info Security Web site, "Infosecurity Europe 2012—The insider threat, is it real?" www.infosecurity-magazine.com/view/25434/infosecurity-europe-2012-the-insider-threat-is-it-real/, accessed June 8, 2012.
[76] Info Security Web site, "Majority of firms plan to institute employee monitoring for social media use," www.infosecurity-magazine.com/view/26098/majority-of-firms-plan-to-institute-employee-monitoring-for-social-media-use, accessed June 8, 2012.

exploitation through their connections to another country and culture and recommends "exercising great sensitivity when vetting foreign born employees."[77]

The workforce in the sciences, technology, engineering, and mathematics fields in particular is becoming more globally distributed. More than 40 percent of the 25,000 doctoral degrees in these fields awarded by U.S. institutions in 2011 went to nonresident students, according to an Economic Modeling Specialists International analysis of data from the National Center for Education Statistics. The more advanced the education level, the higher probability that graduates in the sciences; technology, engineering, and mathematics are foreign-born. About 20 percent of engineering graduates from American universities are foreign-born. At the master's degree level, the percentage is closer to 50 percent, and 56 percent of engineering doctoral grads in 2011 were from abroad.[78] If the current trend continues, and an ever-higher proportion of advanced degrees in the science, technology, engineering and math fields are awarded to foreign-born students, this issue could assume greater urgency.

Global Network Environment

The subject matter experts discussed information network technology developments, which increase productivity but also supplement the malicious insiders' toolkit. This toolkit enables insiders to broaden their playing field and greatly increase their ability to quickly transfer vast amounts of sensitive or proprietary information worldwide with relative anonymity. According to a 2005 report from the Defense Personnel Security Research Center, technological advancements in information storage and retrieval, increasing global demand for protected U.S. information, the internationalization of research and development and commerce, and global Internet expansion have converged to create unprecedented opportunity for insiders to steal and transfer information to foreign entities.[79]

Opportunities

There would be opportunities for public and private critical infrastructure stakeholders to maintain the upper hand in the Advantage Good Guys future.

- Establishing and sharing best practices that are accepted by overseas partners: the workshop participants generally agreed that the United States has not yet been successful in mitigating the global threat to U.S. critical infrastructure. Even if the United States becomes a less vulnerable target in the Advantage Good Guys scenario, it must continue to improve the security of overseas enterprises and operations that affect U.S. critical infrastructure and its supporting supply chain.
- If proper measures are taken to contain or reduce insider threats, companies may spend less on legal fees and insurance.

---

[77] Gelles, Michael, David Brant, and Brain Geffert, *Building a Secure Workforce*. Deloitte Consulting LLP, 2008: 6–7, www.deloitte.com/view/en_US/us/Industries/US-federal-government/764ef33b4010e110VgnVCM100000ba42f00aRCRD.htm, accessed April 25, 2012.

[78] Wright, Joshua, *Economic Modeling Specialists International Blog*, "How Foreign-Born Graduates Impact the STEM Workforce Shortage Debate," May 28th, 2013, www.economicmodeling.com/2013/05/28/how-foreign-born-graduates-impact-the-stem-workforce-shortage-debate/, accessed July 5, 2013.

[79] Kramer, Lisa A., Richards J. Heuer, Jr., and Kent S. Crawford, *Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage*, Defense Personnel Security Research Center Technical Report 05-10, Monterey, CA: Defense Personnel Security Research Center, May 2005: 12.

- Employee insider threat awareness training must continue to evolve.

Signposts and Indicators

The subject matter experts identified the following indicators that the Advantage Good Guys future may be emerging. These indicators can be a signal to public and private critical infrastructure stakeholders.

- Emergence of effective policies that include dialogue, public/private information sharing, standards, performance metrics, and deliverables.
- Adoption of employee privacy laws that specifically address the many facets of mitigating insider threats to physical and cyber assets (primary and supporting) that are deemed as U.S. critical infrastructure.
- Reduction in number of insider attacks (successful and unsuccessful). One facet of this includes successful containment of attacks before significant damage occurs to critical infrastructure.
- Emergence of a "human firewall" through increased awareness, employee training, and well-crafted reporting programs for insider indicators, including behavior, financial stressors, travel, and contacts. Employees would know mechanisms through which they can report such information. The subject matter experts emphasized that increased reporting would not necessarily mean that the insider problem is getting worse, but may simply reflect an increased awareness of it. This will become a critical complement to advanced cyber, technical, and physical security programs.
- Availability of effective insider threat risk-based prevention and detection technology that correlates disparate data sources to potential technical and behavioral indicators of malicious activity while adhering to employee privacy laws.
- Standardized personnel policies that inform stakeholders what to look for and how during screening of applicants and monitoring the workforce, going well beyond static background and criminal checks.
- High-quality, dynamic, formalized education and training on insider threats that is reinforced at all levels of an enterprise, including offering college-level courses for risk managers.

Alternative Future: Mission Impossible

In the Mission Impossible future, the insider is more capable and diverse, making effective risk management more difficult, if not impossible. A haphazard culture of governance sets the scene for repeatable and systemic insider attacks in the "cloud."[80] In this world, an increased number

[80] According to the Committee on National Security Systems, cloud computing is the model for enabling on-demand network access to a shared pool of configurable IT capabilities/resources, e.g., networks, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. See Committee on National Security Systems (CNSS), *National Information Assurance (IA) Glossary*, CNSS Instruction No. 4009, April 26, 2010: 12. The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing

of insiders using technologically enhanced techniques can launch targeted and potentially widespread attacks with impunity from one or multiple vectors with minimal risk of attribution. Outsourcing continually broadens the field of potential adversaries in the U.S. critical infrastructure virtual supply chain. The "high-tech" insiders have a significantly enhanced asymmetric capability to create widespread physical impact though cyber means. Perhaps even more damaging, they can conduct widespread cyber exploitation attacks, the effects of which cannot be readily seen before resulting in potentially catastrophic consequences. The sophisticated insiders in this future become systemic threats because they will continue their malicious activities until someone stops them. In essence, most technologically advanced adversaries do not want to disrupt systems or services that might support their overall plans.

In the Mission Impossible future, cybersecurity may prevent or detect some attacks, but strategic response is limited because an attack may go undetected and is unlikely to be localized or easily attributable. Physical protection systems may be more easily compromised because they are also IP-connected, although with the recent advent and integration of advanced threat detection platforms, attribution becomes feasible.[81] Twenty years from now, a professional will know how to obfuscate and cloak identities in a haphazard governance environment in this future.[82] To this point, the workshop participants noted that even effective governance would be unable to counter the technology-enhanced insider.

Challenges

The subject matter experts outlined the following challenges for public and private critical infrastructure stakeholders in the Mission Impossible alternative future.

- The threat landscape shift as a result of Web 3.0 and "cloud" computing, e.g., "deperimeterization"[83] and the proliferation of proximity attacks[84] as part of the digital insider[85] tactics, techniques, and procedures.

---

resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. See the *NIST Definition of Cloud Computing*, September 2011.

[81] For further discussion see Kellermann, Tom, "The Knight Fork: Defining Defense in 2013," November 2012, www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/op_kellermann_the-knight-fork_defining-defense-2013.pdf, accessed December 7, 2012.

[82] According to the U.S. Government Accountability Office, the number of cybersecurity incidents reported by Federal agencies to US-CERT increased approximately 680 percent between Fiscal Year 2006 and Fiscal Year 2011. US-CERT attributes the increase, in part, to agencies improving their detection and reporting of network security incidents. See U.S. Government Accountability Office, *Cybersecurity: Threats Impacting the Nation*, GAO-12-666T, Washington, D.C.: U.S. Government Accountability Office, April 24, 2012: 9.

[83] A term used by several of the experts supporting this NRE, "deperimeterization" is a term coined by the Jericho Forum to describe the erosion of the traditional 'secure' perimeters, or 'network boundaries,' as mediators of trust and security. These boundaries are not just physical but also logical in the sense that they demarcate the edges of an organization or enterprise. See Dubrawsky, Ida, "The "De-perimeterization of Networks," *Microsoft TechNet*, September 12, 2007, http://technet.microsoft.com/en-us/library/cc512604.aspx, accessed September 10, 2012.

[84] The proliferation of proximity attacks was discussed within the context of a malicious insider being able to exploit technical and human vulnerabilities in a future Web 3.0 world characterized by trust in "cloud" computing and replete with personal wireless, mobile devices in the workplace. As explained in a Cisco Technical Newsletter on wireless network security, the hacker (or for the purposes of this NRE, the "digital insider") does not need to "plug in" to access a network; however, putting the threat in perspective, physical proximity is required to attack a

- Every critical infrastructure and supporting industry is as vulnerable as the weakest member of the supply chain or network to which it is linked. This will become increasingly critical in a future where new operational and cyber-related dependencies expand and distribute the interconnections among infrastructure.
- The Internet virtual "arms bazaar" that gives adversaries increasingly easy access to a wider array of cyberattack tools.
- An ongoing lack of industrial policies and standards to defend against current and future insider threats, without which the interoperability and transfer of information is vulnerable to an attack because the system and data are open for manipulation. Due to the lack of clear policy statements in this future, it is impractical to think that appropriate precautions will be taken to prevent attacks, let alone sophisticated cyberattacks.
- Obtaining well-targeted funding for governance and keeping pace with a rapidly evolving threat. Key in this regard are risk-based and prioritized funding decisions to ensure resources are directed at the most appropriate aspects of the insider threat to a specific infrastructure or supporting asset.
- Globalization of the workforce.
- Striking an appropriate balance between security concerns and employee privacy issues, while effectively dealing with the insider threat.

Based on these challenges, the subject matter experts focused on three major factors that will increasingly de-localize the malicious insider threat in the Mission Impossible future: 1) increased use and dependence upon the "cloud," 2) increased outsourcing to address business inefficiencies and market demands, and 3) increased role of technology in expanding the "converged threat" (cyber and physical) against U.S. critical infrastructure.

The "Cloud"

Most insider threats today are facilitated by information and communications technology, and it is sometimes not the user that is compromised but the device that he or she is using. The "cloud" has expanded the boundaries of critical infrastructure, much as it has the scope and reach of the "digital insider," without being treated and protected as critical infrastructure itself. Trust in the "cloud" increases risk because of increased opportunities for remote access to critical systems. The subject matter experts agreed that malicious "cloud"-use scenarios are frightening because potential impacts could extend well beyond the cyber realm into the physical, for example, in the case cyber-initiated chemical or biological attacks. Over the next 20 years, there will be numerous technological advances that will affect U.S. critical infrastructure whose potential security vulnerabilities will need to be evaluated before fielding on a wide scale. Unfortunately, technology moves quickly and malicious actors are likely to quickly leverage it to suit their needs.

---

wireless network. See Anderson, Neil, *Securing Wireless Networks*, www.cisco.com/web/services/news/ts_newsletter/tech/chalktalk/archives/200802.html, accessed October 3, 2012.

[85] Digital insider refers to the phenomenon of remote access by means of software-based backdoors within a critical system, similar to an advanced persistent threat.

- The term "digital insider" refers to the possibility of remote access via software-based backdoors within a critical system. As remote access increases, with the digital insider beginning to navigate stealthily through the "cloud," employers will need to consider the security of online encryption against advanced adversaries. Considering encryption security is necessary because U.S. critical infrastructure increasingly is connected to the Internet.[86] The ease and impact of insider thefts, because of technological advances in the storage and movement of data, encourages the number of data compromises to increase exponentially.[87]
- The subject matter experts noted that the new-generation workforce may be more emboldened to take risks because they perceive their older supervisors as much less savvy with regard to information technology and, therefore, less likely to realize that anything is amiss. Additionally, remote workers may be more willing and empowered to take risks by virtue of their distance from supervisory control. The subject matter experts cited WikiLeaks as an example of the type of insider threat in a globalized and networked environment, wherein the perpetrator has the opportunity to submit information securely and anonymously. According to a 2011 white paper by Verdasys, a leading cybersecurity firm, the problem with sites such as WikiLeaks is that the "…lack of personal accountability eliminates much of the moral hazard that deters otherwise risk-averse users from exposing sensitive data. With secure sites purpose-built to shelter them, a much wider pool of potential violators can now consider such subversion with little fear of repercussion."[88]

The subject matter experts also discussed the new generation workforce and "deperimeterization" of the future insider threat within the context of the increased likelihood of insider targeted attacks in a Web 3.0 world. Web 3.0 is the next stage of the Internet that becomes a venue for the exchange of dialogue that resembles real life communication. One expert describes the Web 3.0 world as follows:

> "Everything with an electric current running through it has an IP address and is communicating with other machines like it without the need for human intervention. The machines will get to a point approaching artificial intelligence where they will learn about your likes, dislikes and needs, locations and associations and organize and present information to you from the Web. The user must not demonstrate intention as he or she will not need to click on a link or open an attachment anymore to receive information. This is big data driven by the cloud and with the mobile device as your personally tailored endpoint (mobile) which gathers, stores, accesses and transfers this information."[89]

With access such as this in the malicious insider's toolkit, it becomes more critical for the

[86] One subject matter expert noted that a basic Input Output System (BIOS)-level insider attack would nullify any current encryption.
[87] Verdasys, *Protecting Against WikiLeaks Type Events and the Insider Threat,* January 2011: 3, www.iseprograms.com/lib/Verdasys_WikiLeaks.PDF, accessed September 11, 2012.
[88] Verdasys, *Protecting Against WikiLeaks Type Events and the Insider Threat,* January 2011: 2, www.iseprograms.com/lib/Verdasys_WikiLeaks.PDF, accessed September 11, 2012.
[89] Kellermann, Tom, "The Evolution of Targeted Attacks in a Web 3.0 World," July 2, 2012, http://cloud.trendmicro.com/the-evolution-of-targeted-attacks-in-a-web-3-0-world/, accessed August 13, 2012.

physical and cyber security authorities to work together to adapt to a rapidly changing technological threat landscape faster than the adversaries can.

In its 2008 *Disruptive Civil Technologies* report, the National Intelligence Council best characterized this future challenge as "The Internet of Things," information and technology devoted to increased connectivity of people and things that offers the potential to enhance or degrade U.S. economic, political, and military power over the next 15 years.[90] The report assesses that by 2025 Internet nodes may reside in everyday objects and that people may be able to remotely control, locate, and monitor even the most mundane devices and articles. The extent to which even everyday items become information security risks, the "Internet of Things" could distribute those risks more widely than the Internet has done to date.[91]

Outsourcing

Going hand-in-hand with concerns over the "cloud" and the ambiguity of insider threat boundaries are the issues of outsourcing and virtual supply chain threats, which were common themes raised throughout the alternative futures workshop and tabletop exercises for this NRE. Classified and otherwise sensitive information in the "cloud" creates a group of new insiders (subcontractors) with access and the ability to manipulate or give away information no longer stored at home base. With inefficiencies and the marketplace forcing more third-party outsourcing, organizational IT departments will be the first to relocate, along with localized control of how to identify and mitigate insider threats.

Globalization of the workforce will deepen the dependence on outside vendors, leaving every organization as vulnerable as its weakest partner. As this trend increases, the public and private sector will outsource more work with additional subcontracts to carry out their missions. Organizations will need to consider how this impacts their risk, as their work expands and demands a larger workforce.

The "Converged Threat"

Advances in information technology and increasing dependence upon the Internet offer future malicious insiders converged capabilities to conduct targeted physical sabotage within the cyber systems context. These blended attacks where the physical and virtual worlds converge have potentially severe implications for operations and security across all 16 critical infrastructure sectors. Increased insider capabilities aside, the critical change in the Mission Impossible future is the exponential increase in potential vulnerabilities, as economic and technological imperatives drive critical assets from traditionally stand-alone, siloed systems to IP-based networks. In this world, the adversary is better equipped to target critical systems with greater speed and anonymity.

The subject matter experts identified a corollary to the converged threat where the future insider will have a dual threat capability as a result of advanced cyber capabilities and physical

[90] U.S. National Intelligence Council, *Disruptive Civil Technologies: Six Technologies with Potential Impacts on U.S. Interests Out to 2025,* Conference Report CR 2008-07, April 2008: iii, http://www.fas.org/irp/nic/disruptive.pdf, accessed March 15, 2012.
[91] U.S. National Intelligence Council, *Disruptive Civil Technologies: Six Technologies with Potential Impacts on U.S. Interests Out to 2025,* Conference Report CR 2008-07, April 2008: v, www.fas.org/irp/nic/disruptive.pdf, accessed March 15, 2012.

proximity. They suggested that "proximity attacks" will become more frequent as Web 3.0 devices become a critical part of everyone's lives. In this future, a person does not need to be an employee or trusted business partner to be an insider. Twenty years from now, when everyone has network cameras and carries Web 3.0 personal electronic devices, those seeking to do harm can simply use their devices as surrogates or "technical slaves." Because of technology, people's physical presence in a room makes them susceptible, for example, when Bluetooth technology is used to remotely turn on microphones and cameras. The subject matter experts commented that this type of incident could happen right now, which makes the risk landscape of 20 years from now even more disturbing

Opportunities

The subject matter experts outlined two major opportunities for public and private critical infrastructure stakeholders in the Mission Impossible alternative future.

- Converging the physical and cyber security management programs to defeat the advanced insider capabilities. The workshop participants were concerned that it might take a successful insider event to motivate public and private stakeholders and public opinion to marshal resources and resolve long-standing legal and technical roadblocks to more holistic security management.
- Learning from failures and best practices to make the governance of insider risk management more effective. This includes implementing robust threat information sharing and reporting procedures and mechanisms, both vertically and horizontally, among all concerned public and private stakeholders. There must be improvements in making sure the right information reaches the right people at the right time to better deter and detect insider threats.

Signposts and Indicators

The SMEs identified the following indicators that can signal public and private critical infrastructure stakeholders that the Mission Impossible future may be emerging.

- An increase in the number of successful insider attacks.
- An increase in insider attack attempts, as distinct from successful attacks. The environment is conducive to attacks, because the insider knows the vulnerabilities inherent in a haphazard governance culture. By their actions, malicious actors indicate what they view as valuable and critical.
- Insiders that should have been easy to detect and catch but were not.
- Failure to migrate from service-level agreements to best practices for insider threat programs. Organizations are encouraged to migrate to the "cloud" because it increases security, but security against infiltration and insider threats is decreased. "Cloud" providers to critical infrastructure should be considered, by association, critical infrastructure in themselves. Accordingly, they should be held to higher standards than simple service-level agreements, which are prevalent today. Having these standards in place, according to the workshop participants, would represent a fundamental game shift against the malicious insider.
- Lack of oversight and policy regarding outsourcing, particularly in the technical support and source code production arenas. The workshop participants agreed that third parties

and trusted business partners should be held to the same standards as the contracting organization.

- Inconsistent funding for protection standards against insider threats across all U.S. critical infrastructure sectors.
- A continuation of a poor record of logging across all sectors, which typically improves only after incidents have occurred. In this regard, indicators of insider activity (for example, trying to send out large amounts of data or a computer communications with an Internet Protocol (IP) address that does not exist in the Domain Name Server (DNS) cache) will vary depending on the type of infrastructure, the threat, and the intended method of compromise, making them difficult to isolate and analyze based on static rules.
- Ongoing confusion as to what organizations are *allowed* to do with regard to employee privacy and civil liberties.

Table 3 provides a summary of the in-depth findings for the Advantage Good Guys and Mission Impossible alternative futures.

Table 2. Summary of In-Depth Insider Threat Alternative Futures

	Advantage Good Guys	**Mission Impossible**
Challenges	▪ Maintain effective governance in the face of constantly evolving threats ▪ Balance operations and security ▪ Manage relevant data ▪ Retain funding ▪ Monitor "consumerization" of insider threat ▪ Globalization of the workforce ▪ Employee trust as a counterpoint to globalization of the workforce	▪ Web 3.0 and "cloud" computing, e.g., "deperimeterization" of the threat ▪ Interdependencies that render critical infrastructure and supporting industries as vulnerable as the weakest partner ▪ The Internet virtual "arms bazaar" ▪ Lack of policies and standards ▪ Policy, legal, and technical issues associated with obtaining and analyzing relevant threat data ▪ Risk-based funding for governance ▪ Globalization of the workforce ▪ Balancing employee trust and privacy issues
Opportunities	▪ Establish best practices accepted by overseas partners ▪ Potential for lower costs (e.g., legal, insurance) ▪ Employee insider threat awareness training must continue to evolve	▪ Converging the physical and cybersecurity management programs ▪ Learning from failures and best practices

Signposts and Indicators	▪ Performance-based policies that include information sharing, standards, metrics, and deliverables ▪ Reduced number and severity of insider attacks ▪ Increased awareness and reporting on insider activity indicators ▪ Employee privacy laws that specifically address the many facets of mitigating insider threats to physical and cyber assets (primary and supporting) ▪ Emergence of a "human firewall" for reporting on insider activity indicators ▪ Standardized personnel policies ▪ Formalized education and training on insider threats	▪ Increased number of successful insider attacks ▪ Insiders that should have been easy to catch but were not ▪ Increased attack attempts, distinct from successful insider attacks ▪ Failure to migrate from service-level agreements to best practices for insider threat programs with regard to "cloud" providers ▪ Lack of oversight and policy regarding outsourcing, particularly in the technical support and source code production arenas ▪ Inconsistent insider threat funding and protection standards ▪ Continuation of a poor overall record of logging ▪ Confusion as to what organizations are *allowed* to do with regard to employee privacy

Strategic Surprises

The subject matter experts discussed a number of low-likelihood and high-consequence "strategic surprises"[92] that could bring chaos to the insider threat landscape and U.S. critical infrastructure during the next 20 years.

- An insider terrorist cyberattack. For example, an insider at a large industrial or chemical processing plant designs a "logic bomb" to shut down all of the critical valves and/or severely alter the system by simply "commenting out" one line of code. The workshop participants offered that this would not necessarily be a particularly sophisticated attack for the skilled, well-placed insider.
- A widespread "cloud" computing attack.
- Insiders having a direct gateway to the device of their choice via compromise of application ("app") stores, an inevitable threat possibility based on current technology trends and public demand.
- A dramatic drop in cybersecurity funding as a hasty reaction to a devastating physical attack.

[92] A strategic surprise is an unanticipated incident or event that causes significant disruption or damage to a critical infrastructure and/or supply chain. See the U.S. National Intelligence Council, *Disruptive Civil Technologies*, Conference Report CR 2008-07, April 2008: v, www.fas.org/irp/nic/disruptive.pdf, accessed March 15, 2012.

- Contamination of assets and products in the Food and Agriculture, Water and Wastewater, and Healthcare and Public Health Sectors.
- Release of or tampering with harmful chemicals via cyberattack.
- "Logic bombs" planted by systems administrators that impact the Healthcare and Public Health Sector. For example, in one actual incident, a security guard successfully planted a "logic bomb" (downloaded from the Internet) onto hospital computers which could have brought down the hospital's critical HVAC systems.
- An asymmetric weapon attack on a Government Facilities Sector asset to render a symbolic landmark or place unusable for the foreseeable future, thereby creating a profound psychological impact.
- An attack on a key financial clearinghouse that manipulates critical functions, such as the integrity of servers controlling time stamps for high-frequency trading.

Chapter 5: Insider Risk Mitigation: Challenges and Opportunities

Introduction

The U.S. Critical Infrastructure community faces both challenges and opportunities for mitigating current and future insider threats. Existing best practices inform mitigation measures, but the nature of insider threats leads to specific areas that are particularly challenging, in which opportunities exist to increase the effectiveness of current measures against malicious insiders.

During the tabletop exercises supporting this NRE, subject matter experts were asked to respond to and evaluate insider threat scenarios through the Prevent, Protect, Mitigate, Respond, and Recover (PPMRR) framework (Figure 6-1).[93]

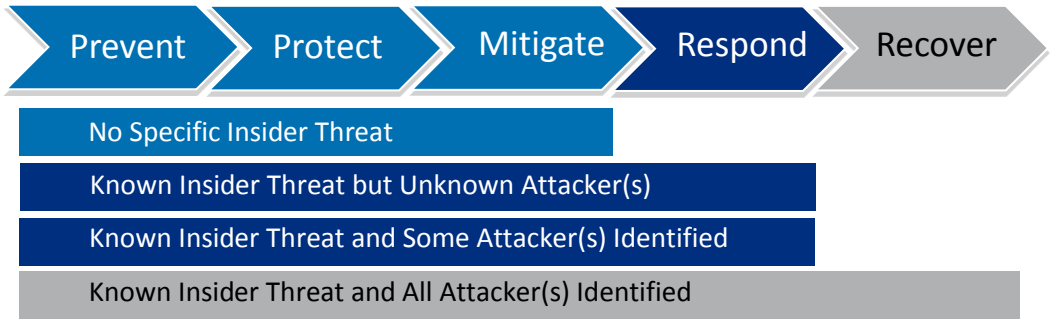

Figure 8. The PPMRR Framework

The subject matter experts agreed on the need to develop and enforce a comprehensive and scalable insider threat program standard for U.S. critical infrastructure as it relates to PPMRR. Ideally, such a standard would include long-term employee monitoring policies that begin with pre-employment background checks, continue with technical and non-technical monitoring and training throughout the employee's tenure at an organization, and extend access policies to post-termination or departure to ensure that proper safeguards are implemented, preventing former employees from accessing sensitive information.

Cross-cutting standards for insider threat programs and initiatives do not exist for all critical infrastructure sectors. The subject matter experts did, however, cite the Nuclear Reactors, Materials, and Waste Sector and Electricity Sub-sector as having insider threat programs that other sectors could emulate. The Nuclear Reactors, Materials, and Waste Sector was repeatedly praised for its culture of security that extends beyond background checks and provides security checks throughout the term of employment. In addition, the subject matter experts asserted that the current and emerging standards of the North American Electric Reliability Corporation (NERC) could be expanded and modified to create sector-specific standards relevant to each critical infrastructure, particularly in terms of identifying "critical infrastructures within critical infrastructures" that could become single points of failure.[94]

---

[93] *DHS National Preparedness Goal*, First Edition, September 2011, provides details on the PPMRR framework. Available at www.fema.gov/pdf/prepared/npg.pdf, accessed August 24, 2012.

[94] Under revised regulatory provisions of the NERC CIP standards CIP-002 through CIP-009, all power suppliers and generators must comply with minimum requirements designed to ensure the reliability of the North American

Despite the strong programs within the Nuclear Reactors, Materials, and Waste Sector and the Electricity Sub-sector, research, data, and analysis suggests that no U.S. critical infrastructure sector, industry, or asset is immune to the full scope of insider threats. Even in sectors with relatively robust prevention programs and guidelines in place, the insider threat is a dynamic and expanding one that cannot be eliminated altogether. Regardless of the policies and technologies in place, it could take only one well-placed insider exploiting an organization's known or "zero-day" vulnerabilities to undermine the integrity of a targeted infrastructure and its supporting insider threat program. Once a comprehensive insider threat program is in place, the system will require continuous testing, validation, and monitoring. The subject matter experts emphasized that testing and verification of established policies and procedures to thwart insider threat are necessary to ensure that key security measures become part of the workplace culture and will provide the expected level of protection.

NERC: Even the Best Face Challenges with Insider Threat Standards

NERC Critical Infrastructure Protection (CIP) Standard 004 requires utilities to provide training and safeguards against employees who might use their position to sabotage or attack the utility. The standard requires:

- **Security Awareness Program. Requires that unauthorized access to cyber critical assets be continuously monitored and documented at least quarterly.**
- **Personnel Training. Requires annual cyber training for personnel identified by the personal awareness program. Training includes proper use of cyber critical assets, physical and electronic access controls to cyber critical assets, proper handling of cyber critical assets, and action plans to recover cyber critical assets and access them following a security incident.**
- **Personnel Risk Assessment. Requires documented personnel risk assessment which includes a seven year criminal check at least every seven years.**
- **Personnel Access. Requires utility to maintain a list of personnel with authorized cyber or physical access to cyber critical assets. The list must be updated within 7 days of a personnel change and reviewed quarterly.**[a]

Unfortunately, NERC-CIP 004 has been one of the most violated CIP standards since its inception in 2007. Each utility company is left to identify their own critical cyber assets, which can prove challenging. Even once the assets are identified, compliance with NERC standards can sometimes lag because of management emphasis on other security or economic issues.[b]

[a] NERC, *"Standard CIP-004-4a: Cyber Security Personnel and Training,"* May 24, 2012: 1–3, www.nerc.com/files/CIP-004-4a.pdf, accessed August 23, 2012.
[b] AlertEnterprise White Paper, *NERC-CIP's Most Wanted: The Top Three Most Violated NERC-CIP Standards,* January 2011: 8 and 10, www.energycentral.com/download/products/AlertEnterprise_NERC-CIP_WP.pdf, accessed August 23, 2012.

bulk electric system (BES). CIP-002 requires the identification and documentation of critical assets, e.g., generating plants, major transmission substations, system control centers, and "black start" resources, as well as associated 'critical cyber assets' (hardware, software and data) deemed essential to reliable BES operation. At the heart of CIP-004 (Personnel and Training) is attempting to safeguard system weaknesses against the insider threat. (Black Start refers to the procedure to recover from a total or partial shutdown of the transmission system that has caused an extensive loss of electricity supplies. This entails isolated power stations being started individually and gradually being reconnected to each other in order to form an interconnected system again. Under emergency conditions, Black Start stations receive electricity supplies from small auxiliary generating plant located on-site.)

The subject matter experts repeatedly emphasized that having insider threat programs on the books is meaningless without mechanisms in place for monitoring, validation, and enforcement to ensure their relevancy and effectiveness in the current threat environment. Mitigation has to be as dynamic and adaptable as the threat. A comprehensive insider threat program cannot be *assumed* to operate successfully without continuous testing and monitoring, the latter which includes observation of people and systems. Employee monitoring begins in the pre-employment phase with an initial background check and generally continues through periodic reinvestigations and/or continuous behavioral monitoring, depending upon the criticality of a specific infrastructure or asset. For systems, network monitoring and analysis are critical to identifying "red flags" measured against legitimate "need-to-know" access.

MITRE Keys to Effective Detection

The MITRE Corporation detailed four keys for effective detection of insiders:

1. **Monitor information gathering, manipulation, and exfiltration activities of trusted insiders.**
2. **Monitor activities at the application (searching and printing) level.**
3. **Pay attention to contextual information about users and the information itself.**
4. **Combine alerts and use them to rank analysts for review.**

Source: Caputo, Deanna, Greg Stephens, and Marcus Maloof, "Detecting Insider Theft of Trade Secrets," *IEEE Security & Privacy*, (Vol. 7, No. 6), November/December 2009: 19.

Challenges and Opportunities for Insider Threat Mitigation

During each exercise, the NRE subject matter experts discussed challenges and opportunities for insider threat mitigation. Over the course of workshops and tabletop exercises, the following six issues were assessed to be particularly challenging for the U.S. government and critical infrastructure owners and operators in their current and future efforts to prevent, protect against, mitigate, respond to, and recover from multi-faceted insider threats:

- Acknowledging and dealing with a pervasive threat;
- Breaching roadblocks to public-private cooperation and information sharing;
- Establishing workforce behavioral and access baselines;
- Implementing effective employee insider threat training programs;
- Incorporating public information campaigns into response and recovery planning; and
- Understanding the psychology of a malicious insider.

Acknowledging and Dealing with a Pervasive Threat

In its May 2012 *Cyberattack Task Force Final Report*, the NERC acknowledged the seriousness, scope, and pervasiveness of the malicious insider threat:

> "Insiders pose the greatest threat, especially if they are working with a Foreign State or other High Level threat Actors, because of their detailed knowledge of system operations and security practices. In addition, they have legitimate physical and electronic access to key systems and the controls designed to protect them. Insider individuals can provide qualitative, technical, or physical assistance to the team

requirements of sophisticated adversaries or pose a unique unilateral threat detection challenge, if acting alone."[95]

Mitigation Measures: Facing Outward or Facing Inward

An organization's mitigation measures generally are outward facing and focus on mitigating the damage of a potential malicious outsider. Insider access allows the actor knowledge of an organization's mitigation strategy and, in most cases, the ability to circumvent it. The current National Institute of Standards and Technology (NIST) Information Security Standards document acknowledges that the recommended security controls do not account for the existence of an advanced persistent threat.[a]

Measures that target malicious insiders are either extensions of mitigation measures targeting outsiders or are separate measures intended to identify insiders. The NIST standards identify several steps that organizations should take to mitigate insider threats to systems. These include:

- **Conduct security awareness training on recognizing and reporting indicators of insider threat.**
- **Correlate input from non-technical sources and audit information to enhance the organization's situational awareness.**
- **Create a separate incident handling capability for insider threat.**
- **Ensure organizational coordination for insider threat incident handling.**
- **Limit the ability of a single person to launch a denial of service (DOS) attack.**

[a] National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53 Revision 4, Gaithersburg, MD: U.S. Department of Commerce, February 2012: 25.

Unfortunately, with few exceptions, such outright acknowledgement is not found across all 16 critical infrastructure sectors. Common characterizations of the malicious insider as a disgruntled employee make it easy to downplay the threat and write it off, either as an operating cost or as too difficult and sensitive to tackle. Employees across the spectrum can have a personal or criminal agenda that prompts them to commit malicious acts. The most dangerous malicious insider is the well-liked employee who performs his or her job competently. Statutory, political, procedural, and privacy issues aside, combating the enemy within (versus the outside adversary) is an uncomfortable proposition at best – it is potentially embarrassing, economically costly, and fraught with landmines for an organization's employee relations and public image.

The insider threat applies in varying degrees to all critical infrastructures in the United States. However, the experts supporting this NRE agreed that the insider threat is typically given lower priority and visibility than other attack vectors. They noted that the cross-cutting nature of insider threat and recent incidents, such as WikiLeaks, have forced government, owners and operators, and contractors to revisit their insider risk mitigation strategies.

Recent surveys indicate that corporate leaders recognize that insiders are responsible for as much as 50 percent of security breaches, according to the 2010 Verizon Business Data Breach Investigations Report. The report suggests that despite this acknowledgement, mitigating the threat is hampered by the tendency for corporations and organizations to trust their employees

[95] Cyberattacks Task Force, North American Electric Reliability Corporation, (NERC), *Cyberattack Task Force Final Report*, May 9, 2012: 9.

and to presume their innocence, rather than watching for red-flag behaviors and access patterns to key information and areas. The same report asserts that organizations often turn to technical solutions, when the best option may be quality management and enforcement of current policies to prevent and mitigate insider attacks.[96]

Breaching Roadblocks to Public-Private Cooperation and Information Sharing

The longstanding issue of cooperation between the public and private sectors in dealing with potential insider threats became a recurring point of discussion during the NRE tabletop exercises. The largely public-private nature of U.S. critical infrastructure necessitates that its adequate protection and security depend upon making concrete and fundamental strides in this arena, both in terms of sharing best practices and expertise and in terms of more robust information and intelligence sharing to include cyber threat intelligence, much of which may be classified. Even so, *mutual mistrust*, *misperception*, and *miscommunication* of the insider threat continue to hamper open communication between the U.S. Government and private owners and operators. Within this context, the subject matter experts agreed that closer cooperation between private corporations and Federal Government agencies that allows the former access to Federal Government background information, watch lists of high-risk individuals, and other potential indicators of an insider threat during initial on-boarding procedures could elevate the standards for hiring and continued employment at critical infrastructure facilities. Conversely, there is a vast amount of untapped data within private organizations about insider activity and incidents that rarely makes its way into the hands of researchers or analysts outside of the affected entity. This type of information may be kept solely within the entity because of fears of revealing organizational weaknesses or specific security measures.[97]

The subject matter experts were careful to point out that a major complicating factor in the public-private relationship is that the Federal Government does not act as a homogenous whole, with each major branch and organization following its own policies, procedures, and processes. This makes interfacing with the U.S. Government even more challenging for the private sector.

Echoing the NIAC's findings, the subject matter experts repeatedly expressed doubt that private owners and operators would be willing to commit wholeheartedly to best practices related to information sharing and employee monitoring if such investments of time and resources are detrimental to efficient operations, brand reputation, and profit. These private entities, including contractors and other trusted foreign and domestic third parties, are unlikely to believe they have the economic incentive to place restrictions on their employees or to institute potentially cost-prohibitive insider threat programs without a clear and present threat or a Federal Government mandate.

Defining a level of acceptable risk within U.S. critical infrastructure sectors involves striking a balance between security investments, potentially invasive and severe protection measures, and efficient operating costs. Owners and operators must determine the cost-effectiveness of

[96] Field, Tom, "Inside the Verizon Breach Report: Latest Trends on How Entities are Breached," August 9, 2010, www.bankinfosecurity.com/inside-verizon-breach-report-a-2826/op-1, accessed July 12, 2012.
[97] Caputo, Deanna, Greg Stephens, and Marcus Maloof, "Detecting the Theft of Trade Secrets by Insiders: A Summary of MITRE Insider Threat Research," *IEEE Security and Privacy*, (Vol. 7, No. 6), November/December 2009: 14-21.

protecting against a *perceived* insider threat. The subject matter experts described a difference in organizational cultures between the public and private sectors in how they approach security. They noted the private sector's reluctance to accept government-imposed standards for invasive and prescriptive vetting, hiring, and network and behavioral monitoring policies for employees of critical infrastructure and associated systems. In order to shift the policies of privately owned infrastructure away from using minimum, cost-effective standards toward implementing best practices and applying a more risk-based lens to insider threats, a combination of regulation and market incentives may be required.

From a cost perspective, several subject matter experts agreed that some of the smaller critical infrastructure providers may not be able to practically obtain and manage security clearances. In addition, larger organizations may have security-cleared staff, but not at the executive level where decisions are made.

Despite the perceived reluctance of owners and operators to report malicious insider incidents, several of the subject matter experts felt strongly that processes should be developed and implemented across all 16 critical infrastructure sectors to capture and share such empirical data.

Accepting Effective Security as a Business Value

Private owners and operators (or trusted third parties) of U.S. critical infrastructure often do not view stringent measures and best practices recommended by their U.S. Government counterparts as cost effective. This may, however, be an antiquated idea as information security becomes a differentiating factor between businesses offering the same services. If a business can assure its customers and clients that it can effectively protect information and infrastructure from outside and inside threat, this will engender trust and attract business rather than detract from the bottom line.

Source: PA Consulting Group Web site, "Managing the Threat of Espionage," April 28, 2011, www.paconsulting.com/our-thinking/managing-the-threat-of-espionage/, accessed May 23, 2012.

Throughout the NRE workshops and tabletops, the participants stressed that major legal and privacy hurdles must be cleared before any robust employee background investigation and monitoring can be adopted and implemented by private sector owners and operators. As outlined in the 2008 NIAC *Final Report and Recommendations on The Insider Threat to Critical Infrastructure*, these legal, policy, and procedural issues include providing owners and operators with statutory access to records, aligning insider threat programs with State and Federal legal frameworks, and establishing a research-based nexus between criminal history and behaviors to protect people from undue discrimination.[98] As noted by the subject matter experts, determining where these functions lie within and among the various agencies involved will be a major challenge, as will determining how these functions and agencies will interact.

Contractors and Trusted Third Parties

Effective PPMRR statutes, policies, and strategies must extend beyond regular employees of U.S. critical infrastructure systems and assets. Throughout the government enterprise, contractors and trusted third parties are granted physical and digital access to sensitive

[98] Noonan, Thomas and Edmund Archuleta, *The National Infrastructure Advisory Council's Final Report and Recommendations on The Insider Threat to Critical Infrastructure*, Washington, D.C.: National Infrastructure Advisory Council, 2008: 36.

information. In the case of U.S. critical infrastructure, it is often the private corporations or third parties who own, operate, and control critical national resources.[99] The subject matter experts participating in the NRE process repeatedly stressed that the public-private nature of the owners and operators associated with U.S. critical infrastructure means that insiders could circumvent any actions taken by the Government to prevent insider threats, if private contracting companies do not share the same security culture as the supported infrastructure or the U.S. Government. This could become a potentially greater challenge if an organization continues its relationship with an existing vendor or contracting company that is acquired or merged into a larger foreign corporation with inadequate security or personnel policies.

Public-Private Cooperation and Information Sharing

The subject matter experts highlighted the frequently cited need for better public-private intelligence sharing and reporting to combat the malicious insider threat as major areas for improvement. In some cases, insider threat reporting is not reaching top decision makers because there is no threshold for response or "redline" that requires further reporting up the chain of command or triggers any follow-up action. These experts also noted that, beyond individual organizations or corporations, there is no central intelligence gathering point where insider incident reporting can be cross-analyzed, thus making cross-sector threat trends and patterns hard to identify. In addition, there are no clear-cut mechanisms in place for sharing information across the public-private boundary.

These concerns are supported by general observations and findings in the NIAC's 2012 *Intelligence Information Sharing Final Report and Recommendations*:

> "Information sharing is perhaps the most important factor in the protection and resilience of critical infrastructure. Information on threats to infrastructure and their likely impact underlies nearly every security decision made by owners and operators, including which assets to protect, how to make operations more resilient, how to plan for potential disasters, when to ramp up to higher levels of security, and how to respond in the immediate aftermath of a disaster."[100]

> ***"No single entity looks at all of this data. It's no one's job to look for patterns. We have luck but no procedural entity to analyze an overwhelming body of data."***
>
> *NRE Tabletop Exercise*

The subject matter experts agreed that there is a large volume of collected data that relate to insider threat and could be useful to the U.S. Government, law enforcement, and critical infrastructure owners and operators. Differences in government and private corporations' reporting methods make a central repository a difficult proposition. Even within the U.S. Government framework, the experts expressed doubt regarding the ability to perform focused analysis on multiple agencies' written reports. Despite the considerable challenges, such a repository would likely be the most effective way to create a national-level vision of the problem and discover commonalities and patterns that currently go undetected.

[99] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 2009: 24–25.
[100] National Infrastructure Advisory Council, *Intelligence Information Sharing: Final Report and Recommendations*, January 12, 2012: ES-1, www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf, accessed August 21, 2012.

"The critical infrastructure imperative is widely recognized; for three years in a row (2009-2011) a Presidential Proclamation has designated December as 'Critical Infrastructure Protection Month.' Still, we find that priority of information sharing with critical infrastructure owners and operators, both within parts of DHS and across the Federal Intelligence Community as a whole, does not appear to be commensurate with the widely acknowledged importance of critical infrastructure to the Nation's economic strength and our citizens' way of life."

Source: National Infrastructure Advisory Council, *Intelligence Information Sharing: Final Report and Recommendations*, January 12, 2012: ES-3, www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf, accessed August 21, 2012.

The NIAC has assessed that marked improvements in intelligence sharing within the Federal Intelligence Community and among the U.S. Government and regions, States, and municipalities, have not been matched in intelligence information sharing among the Federal Government and private sector owners and operators of U.S. critical infrastructure, with a few notable exceptions. The 2012 NIAC report supports subject matter expert assertions that *trust* plays a central role in the cooperation and information sharing of public-private risk management systems. This trust only comes from understanding, valuing, leveraging, and testing partners' unique analytic capabilities and contributions.[101]

Workforce Behavioral and Access Baselines

Organizations cannot identify anomalies if they are unaware of the characteristics that define normal behavior for their employees. Despite this, owners and operators may use technological tools or even create standards without a comprehensive understanding of what abnormal activity looks like within their specific areas of responsibility. A critical component of filling this gap would be to recruit and leverage the expertise of human behavioral specialists. Establishing workforce baselines requires knowledge of the human component of the workforce, including demographics, employee lifecycles and financial status, as well as an understanding of the policy environment, including hiring and security policy. Establishing workforce baselines also requires an understanding of current levels of oversight for different types of employees, and an understanding of physical and data access provisions and controls.[102]

Malicious insiders can often thwart protective measures if they are allowed access to areas or information that is not critical to the performance of their specific job duties.[103] When an insider is granted access beyond their daily scope of responsibility, it allows them to act without raising alarms at any layer of protection. Access controls can, however, have an adverse effect on productivity, particularly in the private sector, if

"We need more time to identify the psychology of an insider to differentiate it from general behavioral delinquency. There are different types of insiders for which there need to be tailored mitigation strategies."

NRE Tabletop Exercise

[101] National Infrastructure Advisory Council, *Intelligence Information Sharing: Final Report and Recommendations*, January 12, 2012: ES1–2, www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf, accessed August 21, 2012.

[102] Gelles, Michael, David Brant, and Brain Geffert, *Building a Secure Workforce*. Deloitte Consulting LLP, 2008: 10, www.deloitte.com/view/en_US/us/Industries/US-federal-government/764ef33b4010e110VgnVCM100000ba42f00aRCRD.htm, accessed April 25, 2012.

[103] Field, Tom, "Inside the Verizon Breach Report: Latest Trends on How Entities are Breached," August 9, 2010, www.bankinfosecurity.com/inside-verizon-breach-report-a-2826/op-1, accessed July 12, 2012.

employees must continually ask to gain access to facilities, systems, or information.[104] Therefore, organizations need to balance an employee's need-to-know with what is required to efficiently accomplish the organization's business.

Millennials: Know Your Workforce

Establishing a workforce baseline should be a dynamic process. New entrants to the workforce from the Millennial generation expect a high degree of information exchange and have a low tolerance for restrictions on social networking. These workers are more willing to share personal information in a public setting and are not disposed to view privacy as a necessity.[a] In addition, Millennials, along with the entire workforce, are shifting to mobile computing devices. A recent Symantec study revealed that 47 percent of survey respondents saw mobile devices as the top security concern for cybersecurity professionals and the increase in social media use as a close second with 46 percent of respondents identifying such sites as a challenge. In addition, companies participating in the Symantec survey indicated that they worried most about insiders carrying out attacks, well-meaning or malicious, using mobile devices or social media.[b]

[a] Trend Micro, *12 Security Predictions for 2012*, Cupertino, CA, 2011: 9.
[b] Symantec, *"2011 State of Security: Global Findings,"* 2011:10,

Employee Training

Echoing findings from the 2008 National Infrastructure Advisory Council study on insider threats, the workshop participants identified employee education and awareness on insider threats and recruitment/cooption as the prevention and mitigation measures with the biggest potential return on investment for critical infrastructure owners and operators, particularly in the private sector.[105] Employee training includes a clear explanation of controls that are designed to prevent such actions from occurring. The controls provide a disincentive for employees to engage in detrimental actions. Training should also include information that reinforces the close relationship between employees and their organization's success or failure.[106] This can engender employee loyalty and may increase their potential willingness to report the questionable behavior and actions by others that threaten the organization and, therefore, its loyal employees.

"Take care of employees. In the Intelligence Community and in government we teach people about insider recruiting. Employees in the private sector need a better understanding of what recruiting looks like…Loyalty should be a required part of the corporate culture."

NRE Tabletop Exercise

Employees used as a monitoring force may be the best way to identify malicious insiders, and they must have access to recurring training to do so

[104] Caputo, Deanna, Greg Stephens, and Marcus Maloof, "Detecting the Theft of Trade Secrets by Insiders: A Summary of MITRE Insider Threat Research," *IEEE Security and Privacy*, (Vol. 7, No. 6), November/December 2009: 14-21.
[105] Noonan, Thomas and Edmund Archuleta, *The National Infrastructure Advisory Council's Final Report and Recommendations on The Insider Threat to Critical Infrastructure*, Washington, D.C.: National Infrastructure Advisory Council, 2008: 6.
[106] PA Consulting Group Web site, "Managing the Threat of Espionage," April 28, 2011, www.paconsulting.com/our-thinking/managing-the-threat-of-espionage/, accessed May 23, 2012.

effectively.[107] Co-workers have the closest day-to-day contact with employees who may have malicious intent or who may be dealing with personal or professional issues that put them at risk. Human Resources personnel can be particularly vital sources of information because they work with an employee throughout their employment life cycle and because they are the first and last people to deal with an employee, enabling them to recognize potential for malicious behavior during employment or after termination.[108] The subject matter experts did note that turning the workforce into behavioral monitors could present significant challenges, especially in tight-knit organizations, where reporting anomalies could be seen as disloyal to colleagues.

Defense in Depth: The Workforce as a Monitor

The 2011 Global Fraud Study found that fraud in the United States is detected primarily by tips from other employees (43.1%), management reviews (14%), and internal audits (11.7%). In contrast, IT security controls only detected a fractional amount (0.6%) of ongoing fraud.

Source: Association of Certified Fraud Examiners, *2012 Global Fraud Study: Report to the Nations on Occupational Fraud and Abuse*, 2012: 9, www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf, accessed July 26, 2012.

Employees frequently receive and sign acceptable use policies prior to handling network resources and may be informed of the threat of potential recruitment by outsiders, but this is often conducted only at new employee orientation and may be cursory or rote with little or no follow-up refresher training. [109] A better understanding of insider recruiting methods and motivations could provide private sector employees more actionable exposure to the problem as well as a greater sense of loyalty and buy-in to the organization's role in national security.

Employee training for insider threat should include "red line" definitions and criteria that oblige them to report suspicious behavior. Once employees report such behavior through clear and functioning mechanisms, they should receive feedback or access to any ensuing and related reports to foster and encourage a corporate culture of security and loyalty.

Public Information

A robust public information strategy is a critical component of response and recovery following insider attacks, particularly those with potentially catastrophic psychological consequences, such as nuclear or radiological events. Following any

"The real consequence of an event may not be that bad, but the perception scares people. A lot of the effort must go into trying to inform the public. We have an obligation to explain to them what the consequences really are."

NRE Tabletop Exercise

[107] Gelles, Michael, David Brant, and Brain Geffert, *Building a Secure Workforce*. Deloitte Consulting LLP, 2008: 10, www.deloitte.com/view/en_US/us/Industries/US-federal-government/764ef33b4010e110VgnVCM100000ba42f00aRCRD.htm, accessed April 25, 2012.
[108] Gelles, Michael, David Brant, and Brain Geffert, *Building a Secure Workforce*. Deloitte Consulting LLP, 2008: 11, www.deloitte.com/view/en_US/us/Industries/US-federal-government/764ef33b4010e110VgnVCM100000ba42f00aRCRD.htm, accessed April 25, 2012
[109] InfoWorld Media Group Special Report, *Insider Threat: Deep Dive: Combating the Enemy Within,* Trend Micro, July 2010: 5.

event, U.S. Government and critical infrastructure owners and operators must be prepared to frame technical realities and influence public perceptions of the damage by executing a comprehensive public information campaign that *educates, informs,* and *delivers* accurate and timely information.

Owners and operators must be prepared to counter erroneous perceptions when insiders have considerable credibility by virtue of their position, skill level, or knowledge. While the real consequences of an insider event may not be devastating, the perception of harm from a large-scale event scares people and may cause them to lose confidence in organizations and entities charged with protecting them. The public holds an innate fear of certain types of attacks, especially nuclear, radiological, and biological or chemical. In these cases, it is particularly important for the U.S. Government and private owners and operators to educate, inform, and deliver accurate information as quickly as possible, even if it involves the difficult task of providing evidence that something does not exist.

The subject matter experts felt strongly that each sector should have a plan established through their public affairs office to work with major media outlets to release whatever details are needed to calm the public and allow recovery operations to proceed.

The consensus among the subject matter experts was that if such an information campaign were executed poorly, there could be significant consequences including public skepticism and an adverse effect on employee morale. The task could be made more difficult by the lack of technical education and knowledge of the average citizen and by special interests (e.g., political, financial and religious) that may attempt to leverage such incidents to suit their specific agendas.

Public Relations in a Crisis: Japan's 'Nuclear Boy'

In the wake of the March 2011 Fukushima nuclear plant catastrophe, an animator in Japan created 'Nuclear Boy' to explain the confusing, complex, and terrifying situation at the Fukushima to children. The cartoon used the analogy of a sick child to represent the plant and explained how doctors were administering 'Nuclear Boy' seawater and boric acid medicine to make him better.[1]

A thoughtful and non-technical public relations campaign following an insider attack, but perhaps with a less juvenile focus than in this example, could be very effective in explaining the consequences of a complex situation and minimizing panic.

Source: Maxwell, Kenneth and Andrew Joyce, "Japan tries humor with 'Nuclear Boy' Fukushima," *The Wall Street Journal*, March 18, 2011, http://blogs.wsj.com/japanrealtime/2011/03/18/japan-tries-humor-with-nuclear-boy-fukushima/, accessed August 21, 2012.

Understanding the Psychology of Insiders

Behavioral psychologists among the subject matter experts expressed concern that the primary focus of most insider threat mitigation programs is technical hardware defenses and training programs even though the core problem is a *human* one. The ability to define and recognize "red flags" in terms of insider ideology, motivation, and behaviors remains a challenge to developing truly comprehensive and preventative insider risk mitigation strategies. A working psychological profile of malicious insiders could help to understand the world from which they operate. It also could help identify and define any "critical pathways" that are common to

malicious insiders that separate their behavioral patterns from those of people who are non-maliciously delinquent. A tool of this sort can tailor more effective insider threat programs by distinguishing key psychological and behavioral patterns of witting insiders versus those who maintain their allegiance to their organization.

Some available research indicates that insiders who commit deliberate attacks have a history of security breaches. There does not seem to be a discernible pattern of abuse, but rather a general willingness to break protocol that could signal mal-intent.[110] Conversely, in some cases an insider may seek to act within established protocols so their activities are not investigated beyond cursory monitoring.[111] In these cases, technological or third party information may be more effective at alerting authorities to malicious intent than psychological analysis. Organizations need to be alert to both possibilities for insider behavior so they can routinely and randomly monitor employees who present "red flag" behavior.

DHS Insider Threat Initiatives and Accomplishments

DHS/NPPD/IP

- "Active Shooter Awareness Virtual Roundtable" (September 27, 2011), which included more than 5000 participants and more than 15,000 downloads. The "Active Shooter program also includes an in-residence course for stakeholders.
- "The Insider Threat Virtual Roundtable" (September 18, 2012)
- *"Insider Threat Mitigation Effective Practices*" (draft) December 2011
- SSA EMO Chemical Security Branch - CFATS (Chemical Facility Anti-Terrorism Standards). Resources and tools include industry best practices covering physical security, cybersecurity, and insider threats.
- Sector Outreach and Programs Division (SOPD) – serves as the National Infrastructure Advisory Council (NIAC) Secretariat

DHS/NPPD/Federal Protective Service (FPS)

- OPERATION Shield: *"In an effort to avert or obstruct potential insider threats as part of terrorist operations and criminal activity in and around federal facilities, the Federal Protective Service (FPS) employs Operation Shield. Operation Shield systematically measures the effectiveness of FPS countermeasures. This includes the effectiveness of FPS' Protective Security Officers in detecting the presence of unauthorized persons and potentially disruptive or dangerous activities."* [http://www.dhs.gov/operation-shield]

DHS/NPPD/Cybersecurity and Communications (CS&C) Analysis Sponsorship

- Sponsors Software Engineering Institute- Carnegie Mellon University (SEI-CMU) CERT Insider Threat Center products, including: *Insider Threat Control: Using SIEM Signature to Detect Potential Precursors to IT Sabotage* (April 2011), *Insider Threat Control*

[110] Field, Tom, "Inside the Verizon Breach Report: Latest Trends on How Entities are Breached," August 9, 2010, www.bankinfosecurity.com/inside-verizon-breach-report-a-2826/op-1, accessed July 12, 2012.
[111] Caputo, Deanna, Greg Stephens, Brad Stephenson, and Minna Kim, *Human Behavior, Insider Threat and Awareness: An Empirical Study of Insider Threat Behavior*, The MITRE Corporation, July 31, 2009: 4.

Demonstration: IT Sabotage – Outsider Collusion (December 2011), *Insider Threat Control: using Centralized Logging to Detect Data Exfiltration Near Insider Termination* (October 2011), *Common Sense Guide to Mitigating Insider Threats 4th Edition (December 2012)*, and *The Insider Threat and Employee Privacy: An Overview of Recent Case Law* (not yet released).

DHS/NPPD/ Cybersecurity and Communications (CS&C) /Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT) Partnerships

- Industrial Control Systems Joint Working group (ICSJWG)
  - 2010 Spring Conference, *"The Silent Risk We are Living With: Insider Threat,"* Pan Kamal, CISA AlertEnterprise, Inc.
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a control system security focus in collaboration with the United States Computer Emergency Readiness Team (US-CERT).
- Cross-Sector Cyber Security Working Group (CSCSWG)

DHS/Science &Technology Directorate/Homeland Security Advanced Research Projects Agency (HSARPA)

The HSARPA mission includes developing technologies to aid in the mitigation of insider threats and providing automated scene awareness.

- Human Factors & Behavioral Sciences Division
  - *"DHS Technology Successes and Initiatives,"* Biometrics Consortium Conference, September 21, 2010. Briefing discusses Insider Threat under "Suspicious Behavior Detection."
- Cyber Security Division
  - *"A Roadmap for Cybersecurity Research,"* November 2009 [http://www.cyber.st.dhs.gov]
  - SINET Innovation Summit, *"What are the Opportunities Available to Obtain Federal Research Funding,"* includes Insider Threat under Broad Agency Announcement11-02 (BAA 11-02) Technical Topic Area 4 (TTA-4) for DHS/Financial Services Sector Coordinating Council (FSSCC)
  - Sponsors Software Engineering Institute- Carnegie Mellon University (SEI-CMU) CERT insider threat products, e.g., *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Sector* (2012) *and Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector* (2004).

DHS/Office Intelligence & Analysis (I&A)

- Counterintelligence Working Group (CI-WG): Working in conjunction with ODNI to establish a CI-focused Insider Threat Program, which includes an IT-enabled audit/monitoring capability and standardized CI awareness training. CI-WG also has developed a CI Program Directive, a CI Implementing Instruction, and a CI Security Classification Guide to codify the Secretary's decision to consolidate DHS CI efforts, integrate Component efforts, and execute an effective DHS-wide CI program. *[Extracted*

from "Statement for the Record of Caryn A. Wagner, Under Secretary and Chief Intelligence office, Office of Intelligence and Analysis, before the Subcommittee on Counterterrorism and Intelligence House Committee on Homeland Security, "the DHS Intelligence Enterprise -Past, Present, and Future," June 1, 2011]

- CISD/SITB Homeland Security Note: *"Insider Threat to Utilities,"* IA-0425-11, July 19, 2011.

DHS/United States Secret Service (USSS)/National Threat Assessment Center

- *Insider Threat Study*: One component of an ongoing partnership between the USSS/National Threat Assessment Center and the Software Engineering Institute's CERT Coordination Center, designed to develop information to help private industry, government, and law enforcement better understand, detect and ultimately prevent harmful insider activity.

DHS/Transportation Security Administration (TSA)

- Programs working in conjunction with DHS/S&T
- Aviation Direct Access Screening Program (ADASP), launched in 2006, subjects workers to random physical screening, as well as screening of their personal affects and any vehicles that access security identification display areas (SIDAs).
- Airside Vulnerability Reduction Team, launched in 2008, improves security on the "tarmac" side of federalized airports through improved coordination between airport, airline, and law enforcement stakeholders. Airside security relies on perimeter and personnel security. To qualify for access to SIDAs, airport workers must submit fingerprints for a criminal background check. They are not, however, subject to universal physical screening upon entry to SIDA areas.
- Known Crewmember Program. From http://www.knowncrewmember.org/Pages/Home.aspx:

  "*Known Crewmember (KCM) is a new risk-based screening system that enables Transportation Security Administration (TSA) security officers to positively verify the identity and employment status of flight-crew members. The KCM system is available for use by participating airlines' pilots, and as of October 1, 2012, flight attendants may also be included in the program. The program expedites flight-crew member access to sterile areas of airports, reduces passenger-screening line congestion, enhances security, and makes airport checkpoint screening more efficient for all who depend on air transportation."*

DHS/U.S. Coast Guard (USCG)

- Through the U.S. Coast Guard Counterintelligence Service (CGCIS), the USCG Intelligence Directorate (CG-2) provides tailored CI support to USCG commands, units, and personnel. It has an active CI awareness and training program that includes insider threats. In addition, the CGCIS chairs the Coast Guard Insider Threat Working Group (formerly established in February 2012), which includes representatives from CI, security, information assurance, human resources, legal, and law enforcement.
- The CGCIS has established an Insider threat Awareness site on the USCG network.

- The CGCIS is implementing an Insider Threat Auditing capability within the USCG.

DHS/Immigration and Customs Enforcement (ICE)/U.S. Citizen and Immigration Service (USCIS)

- Security audit conducted by SEI-CMU CERT for DHS IG (Feb 2011) / *"Examining Insider Threat Risk at the U.S. Citizenship and Immigration Services"* (redacted), OIG-11-33, January 2011.

DHS/Federal Emergency Management Agency (FEMA)

- Employee Awareness Training: Two new Counterintelligence Awareness videos are available for viewing on the FEMA Intranet. These videos serve as a great resource for situational awareness as they depict fictional scenarios of insider and technical threats that potentially face FEMA personnel. Video 1: *Get Smarter, Digital Self Defense – Counterintelligence Awareness to Technical Threats* (For Official Use Only), produced by the Office of the National Counterintelligence Executive (NCIX). Video 2: *Betrayed (the trusted insider)* is a full-length video from the FBI.

Appendix A: Acronyms and Abbreviations

ATF	Alcohol Tobacco and Firearms
CBP	Customs and Border Protection
CCTV	Closed Circuit Television
CIP	Critical Infrastructure Protection
CISO	Chief Information Security Officer
CISSO	Classified Information Sharing and Safeguarding Office
CM	Critical Manufacturing
CMMI	Capability Maturity Model Integration
CMS	Centers for Medicare and Medicaid Services
CMU	Carnegie Mellon University
CNSS	Committee on National Security Systems
CSO	Chief Security Officer
DHS	U.S. Department of Homeland Security
DNS	Domain Name System
DOD	U.S. Department of Defense
DOS	Denial of Service
DOT	U.S. Department of Transportation
DTCC	Depository Trust and Clearing Corporation
ECIP	Enhanced Critical Infrastructure Protection
ECTF	Electronic Crimes Task Force
EHV	Extra High Voltage
EMP	Electromagnetic Pulse
EO	Executive Order
FAA	U.S. Federal Aviation Administration

FATF	Financial Action Task Force
FBI	U.S. Federal Bureau of Investigation
FCC	U.S. Federal Communications Commission
FDA	Food and Drug Administration
FINCEN	Financial Crimes Enforcement Network
FPGA	Field Programmable Gate Array
FS-ISAC	Financial Services Information Sharing and Analysis Center
GAO	Government Accountability Office
GISF	Government Information Sharing Framework
HEU	Highly Enriched Uranium
HFT	High Frequency Trade
HHS	U.S. Department of Health and Human Services
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HMI	Human Machine Interface
HVAC	Heating, Ventilation and Air Conditioning
IATA	International Air Transportation Association
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Computer Emergency Response Team
IED	Improvised Explosive Device
IP	Internet Protocol *or* Office of Infrastructure Protection
ISOO	Information Security Oversight Office
IT	Information Technology
LAN	Local Area Network
MAC	Medicare Administrative Contractors
MCO	Multinational Crime Organization

Mo-99	Molybdenum-99
NERC	North American Electric Reliability Corporation
NIAC	National Infrastructure Advisory Council
NIC	National Intelligence Council
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NITTF	National Insider Threat Task Force
NTSB	National Transportation Safety Board
NRC	Nuclear Regulatory Commission
NRE	National Risk Estimate
NRP	National Risk Profile
NSS	National Security Staff
OMB	Office of Management and Budget
PERSEREC	Defense Personnel Security Research Center
PII	Personally Identifiable Information
PMI	Protective Measures Index
PM-ISE	Program Manager-Information Sharing Environment
PPMRR	Prevent, Protect, Mitigate, Respond and Recover
PR	Public Relations
REE	Rare Earth Elements
RPG	Rocket Propelled Grenade
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TRAM	Terrorism Risk Assessment Model

TSA	Transportation Security Administration
TTP	Tactics, Techniques, and Procedures
UAV	Unmanned Airborne Vehicle
US-CERT	United States Computer Emergency Readiness Team
USPS	United States Postal Service
VBIED	Vehicle Borne Improvised Explosive Device
VM	Virtual Machine
VPN	Virtual Private Network

Appendix B: Glossary of Key Terms

Alternative Future Scenario: Plausible alternative views about how the future may develop *(U.S. National Intelligence Council, Disruptive Civil Technologies, 2008)*

Critical Infrastructure Partner: Those Federal, State, local, tribal, or territorial governmental entities, public and private sector owners and operators and representative organizations, regional organizations and coalitions, academic and professional entities, and certain not-for-profit and private volunteer organizations that share in the responsibility for protecting the Nation's critical infrastructure. *(DHS National Infrastructure Protection Plan, 2009)*

Classified Information Sharing and Safeguarding Office: Established by Executive Order 13587 within the Office of the Program Manager for the Information Sharing Environment to provide sustained, full-time focus on sharing and safeguarding of classified national security information. The office also consults partners to ensure the consistency of policies and standards and seek to identify the next potential problem. *(The White House, Fact Sheet Safeguarding the U.S. Government's Classified Information and Networks, 2011)*

Cloud Computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. *(NIST, The NIST Definition of Cloud Computing, September 2011)*

Consequence: Effect of an event, incident, or occurrence. (*DHS Risk Lexicon, 2011*)

Control Systems: Computer-based systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of types of control systems include SCADA systems, Process Control Systems, and Distributed Control Systems. *(DHS National Infrastructure Protection Plan, 2009)*

Corruption: Securing an advantage through means that are inconsistent with one's duty or the rights of others. *(Security along the Border: The Insider Threat, Deloitte Consulting LLP, 2011)*

Corruption Scenarios: Scenarios that involve crime, bribery of public officials, or fraud to facilitate hostile or criminal activities, including but not limited to drug smuggling, immigration, or use of taxpayer dollars. *(NRE Tabletop Exercises)*

Countermeasure: Action, measure, or device intended to reduce an identified risk. (*DHS Risk Lexicon, 2011)*

Critical Asset: Specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively. *(DHS Risk Lexicon, 2011)*

Critical Infrastructure: Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdictions. There are 16 critical infrastructure Sectors: Chemical; Commercial Facilities; Darns; Defense Industrial Base; Emergency Services; Energy; Financial

Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; and Water and Wastewater Systems. (*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001[USA PATRIOT Act]; Presidential Policy Directive on Critical Infrastructure Security and Resilience[PPD-21], 2013*)

Cyberattacks: An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. *(NIST Glossary of Key Information Security Terms, 2011)*

Cybersecurity: The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. *(DHS National Infrastructure Protection Plan, 2009)*

Dependency: The one-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly. (*National Infrastructure Protection Plan, 2009*)

Deperimeterization: A term coined by the Jericho Forum to describe the erosion of the traditional 'secure" perimeters, or "network boundaries," as mediators of trust and security. These boundaries are not just physical but also logical in the sense that they demarcate the edges of an organization or enterprise. *(Microsoft TechNet, The Deperimeterization of Networks, September 12, 2007)*

Digital Insider: Refers to the phenomenon of remote access via software-based backdoors within a critical system, similar to an advanced persistent threat (APT). *(NRE Tabletop Exercises)*

Employee: Person hired to perform a job usually for wages or salary and normally in a position below the executive level. *(DHS Risk Lexicon 2011)*

Espionage: The practice of spying or using spies to obtain secret or sensitive technology or information about the plans and activities of another organization, including a foreign government or a competing company. *(Adapted from Building a Secure Workforce, Deloitte Consulting LLP, 2008)*

Espionage Scenarios: Scenarios that include both economic and industrial espionage.

(NRE Tabletop Exercises)

Executive Agent for Safeguarding Classified Information on Computer Networks: Established by Executive Order 13587 comprised of senior representatives of Department of Defense and the National Security Agency to develop technical safeguarding policies and standards and conduct assessments of compliance. *(The White House, Fact Sheet Safeguarding the U.S. Government's Classified Information and Networks, 2011)*

Exploitation Attack: An attack on critical infrastructure that is focused on exploiting and working within a functioning system to achieve nefarious ends rather than destroying critical nodes for ideological or symbolic purposes. *(NRE Tabletop Exercise)*

Factor: Relative direction of an uncertainty that will shape alternative future scenarios. (*NRE Scenario Workshop Guidance, 2010*)

Homeland Security: A concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. (*DHS Risk Lexicon, 2011*)

Hypervisor: The hypervisor, also called a virtual machine (VM) manager, serves as the control panel ("brain") of the virtualized "cloud" infrastructure, allowing multiple operating systems (OS) to share a single hardware host. The hypervisor is a layer of abstraction between VMs and the underlying hardware, allowing for the dynamic allocation of system resources. Although each OS appears to have the host's processor, memory, and other resources all to itself, the hypervisor actually controls the host processor and resources, allocating what is necessary to each OS and ensuring that the VMs do not disrupt one another. (*Trend Micro White Paper, Changing the Game for Anti-Virus in the Virtual Datacenter, September 2012*)

Improvised Explosive Device: Device placed or fabricated in an unconventional manner that incorporates in its design explosives or destructive, lethal, noxious, pyrotechnic, or incendiary chemicals. *(DHS Risk Lexicon, 2011)*

Industrial Control System: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems (SCADA) used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes. *(NIST Glossary of Key Information Security Terms, 2011)*

Information Sharing: Exchange between entities or individuals of data, information or knowledge stored within discrete information systems or created spontaneously using collaborative communication technologies. *(DHS Risk Lexicon, 2011)*

Infrastructure: The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole. Consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements. (*National Infrastructure Protection Plan, 2009; DHS Risk Lexicon 2011*)

Insider Threat:

- The insider threat to critical infrastructure is one or more individuals with the access and/or insider knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with intent to cause harm. *(NIAC Final Report and Recommendations on The Insider Threat to Critical Infrastructure, 2008)*
- The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. *(National Insider Threat Task Force)*

Interdependency: Mutually reliant relationship between entities (objects, individuals, or groups). (*DHS Risk Lexicon, 2011*)

Inter-Virtual Machine Attack: Inter-VM attacks involve individual virtual machines attacking other virtual machines. This is problematic because most cybersecurity technologies have no visibility into what occurs within virtual machines. (*Trend Micro White Paper, Changing the Game for Anti-Virus in the Virtual Datacenter, September 2012*)

Key Resources: Publicly or privately controlled resources essential to the minimal operations of the economy and government. (*DHS Risk Lexicon, 2011*)

Kinetic Attack: An attack using weapons that rely on energy–blast, heat, and fragmentation, for example–to cause their damage. *(DOD Strategic Command Missions Rely on Space, 2003)*

Likely: Greater than even chance of occurrence. (*Office of the Director of National Intelligence, Explanation of Estimative Language, 2007*)

Likelihood: Chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies, or probabilities. (*DHS Risk Lexicon, 2011*)

Mitigation: Includes those capabilities necessary to reduce loss of life and property by lessening the impact of disasters. It is focused on the premise that individuals, the private sector, communities, critical infrastructure, and the Nation as a whole are made more resilient when the consequences and impacts, the duration, and the financial and human costs to respond to and recover from adverse incidents are all reduced. (*DHS National Preparedness Goal, 2011*)

National Insider Threat Task Force: Established by Executive Order 13487 to develop a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices within agencies. *(Executive Order 13587, 2011)*

National Security: Comprehensive program of integrated policies and procedures for the Departments, agencies, and functions of the United States Government aimed at protecting the territory, population, infrastructure, institutions, values, and global interests of the Nation. (*DHS Risk Lexicon, 2011*)

Network: Group of components that share information or interact with each other in order to perform a function. (*DHS Risk Lexicon, 2011*)

NRE Analysis and Coordination Phase: Concludes the drafting of the NRE and demands an interagency effort to review the NRE for soundness, consistency, and accuracy. This phase includes an assessment of the risks to critical infrastructure from insider threat and helps identify key insider threat trends gleaned from the research and workshop/exercises results. During this phase, the analysis also identifies potential strategies that could mitigate the insider threat to U.S. critical infrastructure. The public or private sector could consider these strategies. *(2012 National Risk Estimate Terms of Reference)*

NRE Research and Planning Phase: Includes a literature review, development of the Terms of Reference document, consultation with subject matter experts about development of insider threat scenarios, and planning for the NRE workshops/tabletop exercises, including contacting and arranging for the participation of appropriate subject matter experts in the workshops/exercises. *(2012 National Risk Estimate Terms of Reference)*

NRE Workshops and Exercises Phase: Includes conducting an alternative futures workshop and three tabletop exercises addressing various aspects of insider threat and U.S. critical infrastructure.

- The alternative futures workshop develops information for the outlook chapter of the NRE. The methodology underpinning the alternative futures development is drawn from the methodology used by the Office of the Director of National Intelligence's National Intelligence Council in their *Global Trends 2025* National Intelligence Estimate and described in a 2008 NIC report on disruptive civil technologies.[112] This methodology was also used as the basis of information for the outlook section of the two previous NREs–*Risks to U.S. Critical Infrastructure from Supply Chain Disruptions* (2010) and *Risks to U.S. Critical Infrastructure from GPS Disruptions* (2011).
- The three one-day tabletop exercises address the three insider threat themes being considered in this NRE–terrorism, espionage, and corruption. Each exercise involves a Red Team exploiting vulnerabilities and developing 4-5 attack plans and a Blue Team developing a response to each of the attack plans to prevent, protect from, mitigate, respond to, and recover from the attack. The exercises provide insights into adversary planning and decisionmaking. *(2012 National Risk Estimate Terms of Reference)*

Owners and Operators: Those entities responsible for day-to-day operation and investment in a particular asset or system. *(DHS National Infrastructure Protection Plan, 2009)*

Prevention: Includes those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. *(DHS National Preparedness Goal, 2011)*

Protection: Includes capabilities to safeguard the homeland against acts of terrorism and man-made or natural disasters. It is focused on actions to protect the citizens, residents, visitors, and critical assets, systems, and networks against the greatest risks to our Nation in a manner that allows our interests, aspirations, and way of life to thrive. *(DHS National Preparedness Goal, 2011)*

Private Sector: Individuals, and entities, including for-profit and non-profit, which are not part of any government. (*DHS Risk Lexicon, 2011*)

Recovery: Includes those capabilities necessary to assist communities affected by an incident in recovering effectively. It is focused on a timely restoration, strengthening, and revitalization of the infrastructure; housing; a sustainable economy; and the health, social, cultural, historic, and environmental fabric of communities affected by a catastrophic incident. (DHS *National Preparedness Goal, 2011*)

[112] U.S. National Intelligence Council, *Disruptive Civil Technologies: Six Technologies with Potential Impacts on U.S. Interests Out to 2025*, Conference Report CR 2008-07, April 2008, www.fas.org/irp/nic/disruptive.pdf, accessed March 12, 2012.

Redundancy: Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process. (*DHS Risk Lexicon, 2011*)

Relative Risk: Measure of risk that represents the ratio of risks when compared to each other or a control. *(DHS Risk Lexicon, 2011)*

Resilience: Ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption. The ability of systems, infrastructures, government, business, communities, and individuals to resist, tolerate, absorb, recover from, prepare for, or adapt to an adverse occurrence that causes harm, destruction, or loss. (*DHS Risk Lexicon, 2011*)

Response: Includes those capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred. It is focused on ensuring that the Nation is able to effectively respond to any threat or hazard, including those with cascading effects, with an emphasis on saving and sustaining lives and stabilizing the incident, as well as rapidly meeting basic human needs, restoring basic services and community functionality, establishing a safe and secure environment, and supporting the transition to recovery. *(DHS National Preparedness Goal, 2011)*

Risk: Potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. (*DHS Risk Lexicon, 2011*)

Risk Assessment: Product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making. (*DHS Risk Lexicon, 2011*)

Risk Management: Process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost. (*DHS Risk Lexicon, 2011*)

Risk Management Strategy: Course of action or actions to be taken in order to manage risks. (*DHS Risk Lexicon, 2011*)

Risk Mitigation: Application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences. (*DHS Risk Lexicon, 2011*)

Risk Mitigation Option: Measure, device, policy, or course of action taken with the intent of reducing risk. (*DHS Risk Lexicon, 2011*)

Sabotage: Action to hinder normal operations, or the deliberate act of destruction or disruption in which equipment or a product is destroyed. *(Building a Secure Workforce: Guard Against Insider Threat, Deloitte Consulting LLP, 2008)*

Scenario: Hypothetical situation comprised of a hazard, an entity impacted by that hazard, and associated conditions including consequences when appropriate. (*DHS Risk Lexicon, 2011)*

Sector: A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. DHS considers 16 critical infrastructure Sectors: Chemical; Commercial Facilities; Darns; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; and Water and Wastewater

Systems. (*National Infrastructure Protection Plan, 2009; Presidential Policy Directive on Critical Infrastructure Security and Resilience [PPD-21], 2013*)

Sector-Specific Agency: Federal departments and agencies identified in PPD-21 as responsible for critical infrastructure protection activities in specified critical infrastructure sectors. (*National Infrastructure Protection Plan, 2009; Presidential Policy Directive on Critical Infrastructure Security and Resilience [PPD-21], 2013*)

Sector-Specific Plan: Augmenting plans that complement and extend the NIPP Base Plan and detail the application of the NIPP framework specific to each critical infrastructure sector. SSPs are developed by the SSAs in close collaboration with other sector partners. (*National Infrastructure Protection Plan, 2009*)

Senior Information Sharing & Safeguarding Steering Committee: Established by Executive Order 13587 co-chaired by OMB and NSS with overall responsibility for fully coordinating interagency efforts and ensuring that Departments and Agencies are held accountable for implementation of information sharing and safeguarding policy and standards. *(The White House, Fact Sheet Safeguarding the U.S. Government's Classified Information and Networks, 2011)*

Severity: Extent of the harm caused by the disruption to the service, and it reflects a consideration of three parts: capacity, substitutability, and extent (geographic and functional). *(2011 National Risk Estimate)*

Steady-State: In the context of the NIPP, steady-state is the posture for routine, normal, day-to-day operations as contrasted with temporary periods of heightened alert or real-time response to threats or incidents. *(DHS National Infrastructure Protection Plan, 2009)*

Strategic Surprise: Unanticipated incident or event that causes or results in significant disruption or damage to a critical infrastructure sector and/or its supply chain. (*U.S. National Intelligence Council, Disruptive Civil Technologies, 2008*)

Subject Matter Expert: Individual with in-depth knowledge in a specific area or field. (*DHS Risk Lexicon, 2011*)

Supervisory Control and Data Acquisition (SCADA): A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (delays, data integrity, etc.) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated. *(NIST Glossary of Key Information Security Terms, 2011)*

System: Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose. (*DHS Risk Lexicon, 2011*)

Terrorism: Premeditated, politically motivated violence perpetrated against noncombatant targets by groups or clandestine agents. *(U.S. Code Title 22, Section 2656f(d))*

Terrorism Scenarios: Scenarios that include physical attacks and cyberattacks against critical infrastructure. *(NRE Tabletop Exercises)*

Threat: Natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property. (*DHS Risk Lexicon, 2011*)

Uncertainty: The areas in each alternative futures scenario that will be of significant importance to insider threat and the CIKR sectors in the coming 20 years. (*NRE Scenario Workshop Guidance, 2012*)

US-Computer Emergency Readiness Team (US-CERT): A partnership between the Department of Homeland Security and the public and private sectors, established to protect the Nation's Internet infrastructure. US-CERT coordinates defense against and responses to cyberattacks across the nation. *(NIST Glossary of Key Information Security Terms, 2011)*

Virtual Machine (VM): A software implementation of a physical computing environment in which an operating system or program can be installed or run. The software resides as protected memory space, usually on a hard disk, and mimics the actions of a central processing unit (CPU) or other hardware devices in using a computer's resources. Requests for CPU, memory, hard disk, network and other hardware resources are managed by a virtualization layer (e.g., a hypervisor) which translates these requests to the underlying physical hardware. *(www.businessdirectory.com and searchservervisulaization.techtarget.com)*

Vulnerability: Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. (*DHS Risk Lexicon, 2011*)

Vulnerability Assessment: Product or process of identifying physical features or operational attributes that renders an entity, asset, system, network, or geographic area susceptible or exposed to hazards. Vulnerability assessments can produce comparable estimates of vulnerabilities across a variety of hazards or assets, systems, or networks. (*DHS Risk Lexicon, 2011*)

Web 3.0: The next stage of the Internet, an Internet for machines where everything with an electric current running through it has an IP address and is communicating with other machines like it, without the need for human intervention. This is big data, driven by the "cloud" and with the mobile device as your personally tailored endpoint that gathers, stores, accesses, and transfers this information. (*Tom Kellermann, Trend Micro, Evolution of Targeted Attacks in a Web 3.0 World, July 2, 2012).*

Zero-day Exploit: A cyber threat taking advantage of a security vulnerability on the same day that the vulnerability becomes known to the general public and for which there are no available fixes. Used in the NRE as zero-day vulnerabilities or exploit or exploit code or attack. *(GAO, Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed, July 2010)*

Appendix C: Risk Assessment Methodology

Introduction

The scenario-based risk assessment methodology is designed to reflect the NRE's high-level scope and the nature of supporting data available to inform the risk assessment. The methodology employs a mix of both qualitative and quantitative approaches, which are consistent with DHS accepted security risk assessment practices specified in the National Infrastructure Protection Plan (NIPP). These techniques are also adapted from leading risk assessment models and approaches such as Military Standard 882 and the Terrorism Risk Assessment Model (TRAM). In addition, key considerations include the lessons learned and best practices gained from the prior NRE efforts, namely the 2011 NRE: *Risks to U.S. Critical Infrastructure from Global Positioning System Disruptions* and the 2010 NRE: *Risks to U.S. Critical Infrastructure from Global Supply Chain Disruptions*. This balanced approach is used throughout this NRE to ensure that the risks from insiders within the United States are assessed and evaluated in an informed and analytically sound manner.

The methodology does not account for the amount of time, effort, resources, and funding needed for risk management, nor who is best suited to carry out the risk management activities. In addition, the scenarios identified and analyzed in this report are a representative sample of potential insider attacks and are not a comprehensive set. Figure C-1 below provides a simplified representation of the insider threat risk assessment methodology.

Figure C-1. Insider Threat Risk Assessment Methodology

Insider Threat Scenario Selection

A literature review and additional research across each of the 16 critical infrastructure sectors using open source material provided the information for developing an initial set of scenarios. Several well-documented scenarios were also prepared from additional detailed research. In addition, the scenarios for this NRE leveraged those developed for previous NREs. The literature review also highlighted three insider themes–terrorism, espionage, and corruption/crime.[113] Scenarios were developed for as many of the 16 critical infrastructure sectors and three attack modes as possible.

[113] For purposes of this risk assessment, terrorism scenarios include physical attacks and cyberattacks against critical infrastructure, espionage scenarios include economic and industrial espionage, and corruption scenarios involve crime, bribery of public officials or fraud to facilitate hostile or criminal activities including but not limited to drug smuggling, immigration, or use of taxpayer dollars.

The consequences for each scenario were assessed using available data and the consequence disruption categories in Table C-3 (end of this Appendix). The final set of scenarios (Table C-4, at the end of this Appendix) were identified as those with a rating of "high" or "catastrophic" in at least one of the scale's six categories. Scenarios that did not receive at least one high or catastrophic rating were excluded from further analysis for the purposes of this NRE.

Vulnerability Assessment

The vulnerability of the targets associated with each of the scenarios was assessed qualitatively using a high-medium-low scale on the vulnerability factors of countermeasure effectiveness and robustness. Each factor was scored individually and could be re-scored after a group discussion resulting in a final vulnerability rating for each of the two factors for each scenario.

When evaluating the **countermeasure effectiveness** factor, the following types of questions were considered:

- Do the countermeasures deny the threat from reaching its target?
- Do the countermeasures detect the threat during or prior to the attack?
- Do the countermeasures interdict the threat during or just prior to the attack?

When evaluating the **robustness / resistance** factor, the following types of questions were considered:

- Does the asset or system have inherent features that immunize it from the attack? (For example, steel structures are stronger than wood structures.)
- Does the asset or system have structural features that immunize it from the attack? (For example, I-beam bridge structures are more rigid than rectangular beam bridge structures.)
- Does the asset or system have redundancies that minimize the impact from the attack? (For example, a telecommunications network with an effective rerouting capability in case a particular hub is disabled from an attack.)
- Does the asset or system have standoff distance protection from a secure perimeter? (For example, an unprotected building inside a secure compound may gain a degree of protection from an IED attack because of the standoff distance created by the secured perimeter.)

The assessment for each scenario is based on a generic asset as opposed to a specific asset. This assumption enabled an assessment of an insider's ability to overcome countermeasures that may be in place to prevent or mitigate an attack. Assessments were based on knowledge about each sector, available data, and information on security countermeasures. Assessments also leveraged DHS data for judgments about target vulnerability for the terrorism scenarios.

Adversary Selection

The intent and capabilities of an insider can dramatically affect the risk assessment for any of the scenarios. Therefore, this assessment considered the characteristics of a generic insider adversary as an individual who is determined, moderately skilled, and capable of planning and

executing a relatively complex attack. This definition was used to develop scenarios and evaluate countermeasure effectiveness for vulnerability scores.

Consequence Assessment

For the purposes of this NRE, consequence represents the expected adverse impact from an attack. The consequences for each scenario were assessed using the criticality scales and definitions that were adapted from those in the DHS TRAM model (Table C-1).

Table C-1. Definitions of Insider Threat Consequence Factors
The contents of this table are UNCLASSIFIED

Criticality Factor	Definition
Business Continuity	The degree of mission disruption in a sector due to interference, manipulation, exploitation, or contamination of a sector's processes as caused by an insider attack/event.
Casualty Impact	The loss of life associated with an event or disruption caused by an insider attack.
Economic Impact	The extent to which an insider event/attack in a sector causes disruption, degradation, or manipulation that affects the livelihood, resources, or wealth of individuals and businesses in a region or the nation.
Emergency Response Function	The extent to which an insider event/attack in a sector causes disruption, degradation, or manipulation of the ability of national- or regional-level emergency services to respond to affected locations.
National Strategic Importance	The extent to which an insider event/attack in a sector affects national security and government continuity.
Replacement Costs	The capital investment required to maintain and support the continuity of the sector as well as the costs associated with repairing, restoring, or replacing the infrastructure targeted by the insider event/attack.

The consequence scores were estimated by rating the impact of each scenario against each of the six consequence disruption factors and assigning a value from 1 to 10. The upper limit (rating of 10), which was provided for each consequence factor, was used to estimate ratio values for each factor's consequence (Table C-2). The consequence assessment considered the question, "*Given the scenario, what is the worst reasonable impact in each of consequence categories?*" Consequence ratings were informed by available open source information and the qualitative vulnerability assessment ratings. For example, the countermeasure effectiveness rating and robustness rating for a particular scenario was taken into account when assessing the consequence factors.

Table C-2. Upper Limits of Insider Threat Consequence Factors
The contents of this table are UNCLASSIFIED

Impact Category	Upper Limit (10)
Business Continuity	Severe degradation or disruption of sector mission fulfillment.
Casualty Impact	Destruction/disruption that could result in over 10,000 fatalities.
Economic Impact	Direct/indirect costs over $100 billion.
Emergency Response Function	Severe degradation or disruption of ability of Federal government to respond at National level.
National Strategic Importance	Severe potential for loss of continuity of government or military operations.
Replacement Costs	Replacement cost in excess of $100 billion.

The scores for each impact category for each scenario were aggregated in a multi-criteria decision analysis based on no weighting of categories (even distribution across the six impact categories) (Figure C-2). Table C-4 (end of Appendix) provides a description of each scenario.

Multi-Criteria Decision Analysis Dashboard

	Scenario	BC	CI	EI	ERF	NSI	RC	Weighted Score
1	Scenario 23	10	8	10	4	8	6	76.7
2	Scenario 29	8	4	8	6	8	8	70.0
3	Scenario 2	8	6	8	4	8	6	66.7
4	Scenario 3	8	6	8	4	8	6	66.7
5	Scenario 21	8	6	8	4	8	6	66.7
6	Scenario 1	8	6	8	4	8	5	65.0
7	Scenario 20	8	6	8	4	8	5	65.0
8	Scenario 31	8	6	8	4	8	5	65.0
9	Scenario 10	6	6	8	4	8	6	63.3
10	Scenario 19	8	6	8	4	8	4	63.3
11	Scenario 24	8	6	8	4	8	4	63.3
12	Scenario 25	8	6	8	4	8	4	63.3
13	Scenario 28	8	2	8	2	8	8	60.0
14	Scenario 5	8	2	10	2	8	4	56.7
15	Scenario 12	6	2	8	6	6	6	56.7
16	Scenario 18	8	2	10	2	8	4	56.7
17	Scenario 26	6	2	8	4	8	6	56.7
18	Scenario 7	4	6	6	3	8	6	55.0
19	Scenario 27	7	2	8	4	6	6	55.0
20	Scenario 15	8	6	6	2	4	6	53.3
21	Scenario 22	4	4	6	4	8	6	53.3
22	Scenario 6	6	2	10	2	6	4	50.0
23	Scenario 4	4	2	8	4	4	6	46.7
24	Scenario 9	8	2	6	2	6	4	46.7
25	Scenario 11	8	2	6	2	4	6	46.7
26	Scenario 13	4	6	4	4	8	2	46.7
27	Scenario 14	8	4	6	2	4	4	46.7
28	Scenario 17	8	2	6	2	4	6	46.7
29	Scenario 8	8	2	6	2	4	4	43.3
30	Scenario 16	4	2	8	2	4	6	43.3
31	Scenario 30	4	2	8	4	4	2	40.0

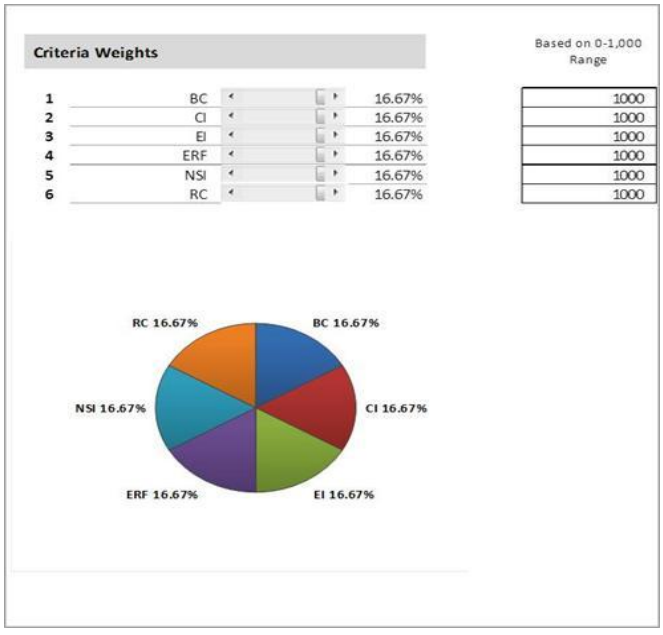

Figure C-2. Multi-Criteria Decision Analysis (No Weighting) for Consequence Assessment by Scenario

Likelihood Assessment

A likelihood rating was estimated for each of the scenarios using a two-step process:

- The scenarios were ranked from most likely to least likely to occur. The likelihood assessment involved estimating the likelihood of a given attack being attempted by an insider relative to the other scenarios with the rank of 1 being assigned to the scenario "most likely to occur." Assigned rankings could be revised after discussion with the objective of obtaining a consensus final rank order (Figure C-3).

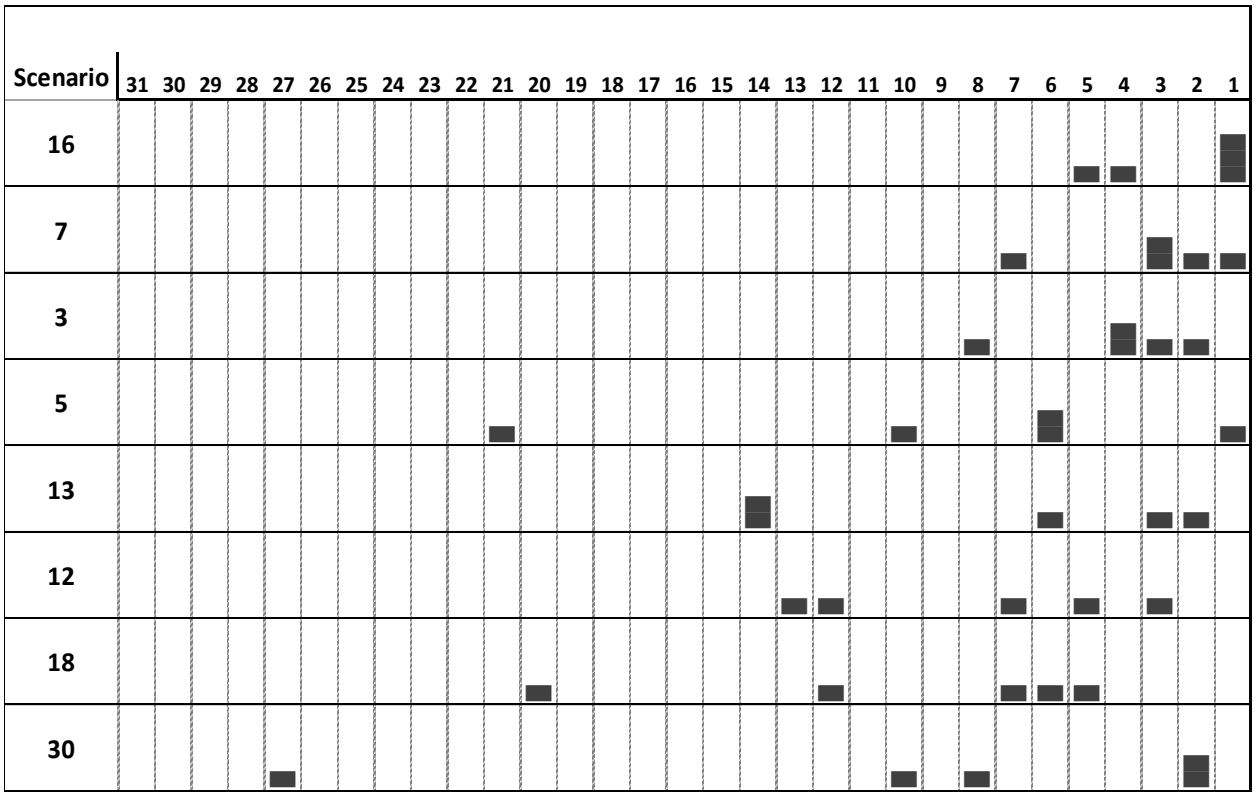

Figure C-3. Distribution of Likelihood Rank Scores by Scenario - Sample

- In the second step of the likelihood assessment, the range of the relative frequency of occurrences for each scenario was estimated. For calculation purposes, these values were converted into a common unit and aggregated to show the minimum, maximum, and median scores. The initial estimate of relative frequency ranges could be revised after discussion with the objective of obtaining a consensus final estimated relative frequency range for each scenario.

Uncertainty

Likelihood assessments incorporate unclassified threat reporting where available. Since threat reporting primarily covers international terrorist threats, and since insider attacks can stem from a number of non-terrorist causes, threat is not considered as its own variable in this assessment, but rather, in tandem with vulnerability. Other considerations include relative frequency of occurrence, plausibility of the scenario, severity of the attack, and potential mitigating factors. These high-level likelihood ratings reflect the uncertainty inherent in estimating the likelihood of insider incidents (Figure C-4).

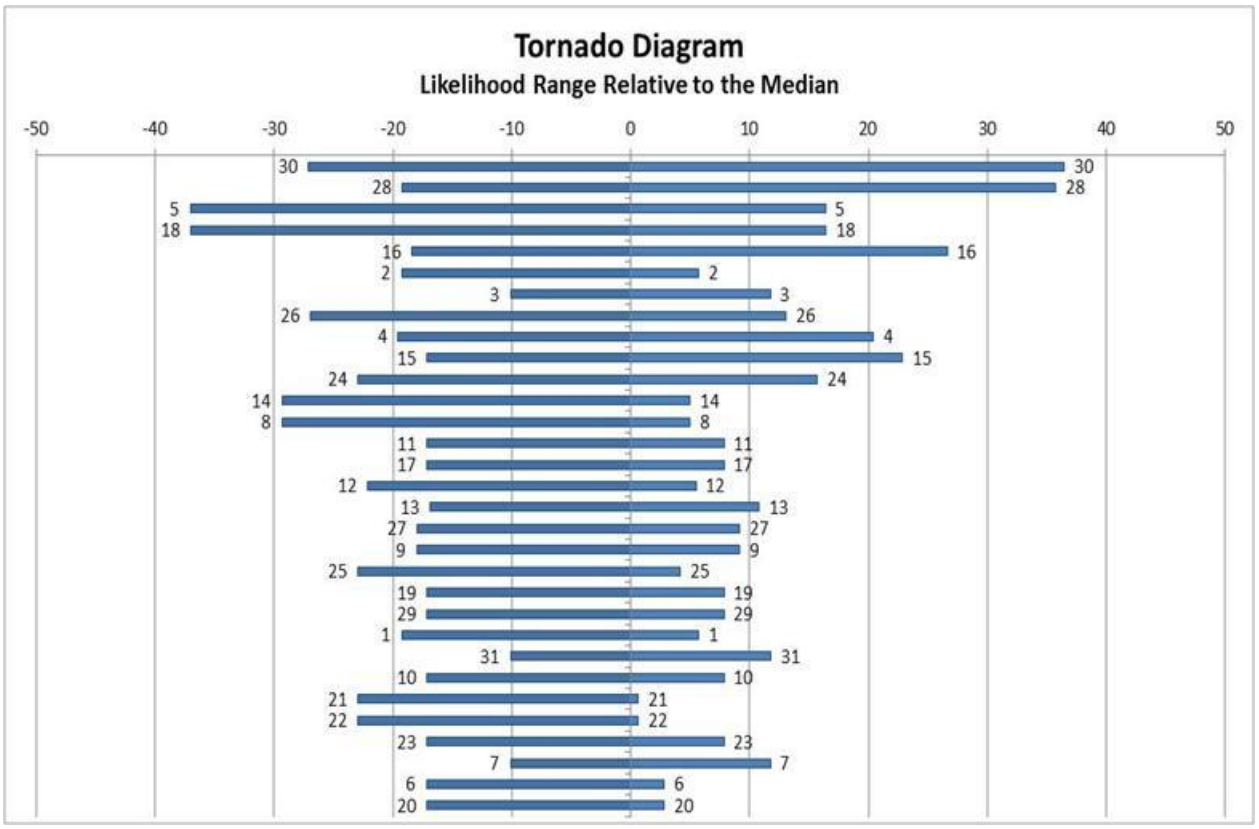

Figure C-4. Tornado Diagram – Analysis of Uncertainty in Likelihood

Monte Carlo Simulation

A Monte Carlo simulation uses a random sampling of data to calculate results based on a probability distribution. It is often used to simulate mathematical models and is ideal for models with small sample sizes. For this reason, a Monte Carlo simulation was chosen to further analyze the risk results. For this risk model simulation, the range of consequence scores for each scenario and the range of likelihood scores were used as inputs. Probability distributions were assigned to these inputs, and a simulation was conducted to obtain the expected value (mean) and standard deviation. Figure C-5 displays the consequence versus likelihood for each sector/scenario combination.

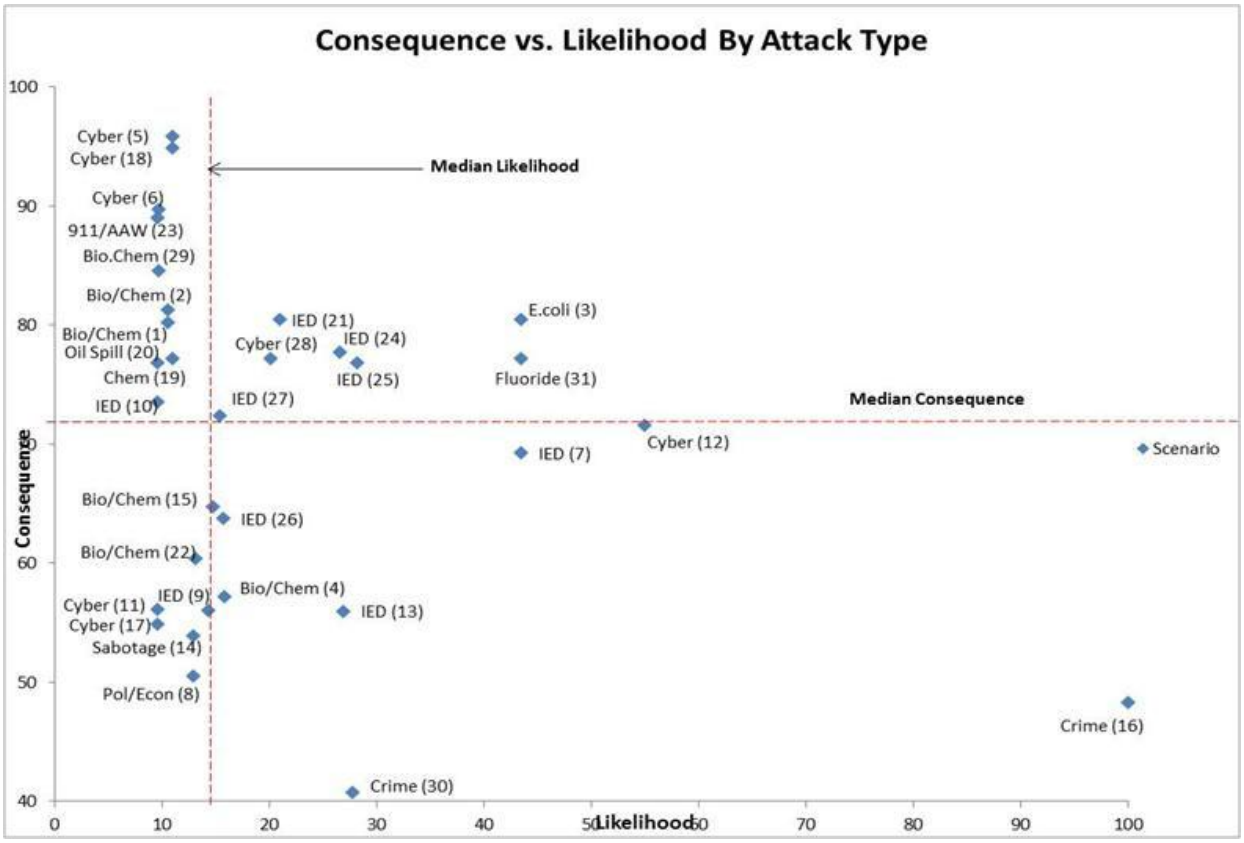

Figure C-5. Relative Risk Diagram

Risk Calculated with Raw Data

The initial risk score was a simple function of the consequence and likelihood scores. Another Monte Carlo simulation was conducted with the range of risk scores as the inputs for each scenario. The simulation produced an expected value for risk with standard deviation. A graphical depiction of the normal distribution risk scores with the range and 95 percent expected value box is shown in Figure C-6. Table C-4 (end of this Appendix) provides a description of each scenario.

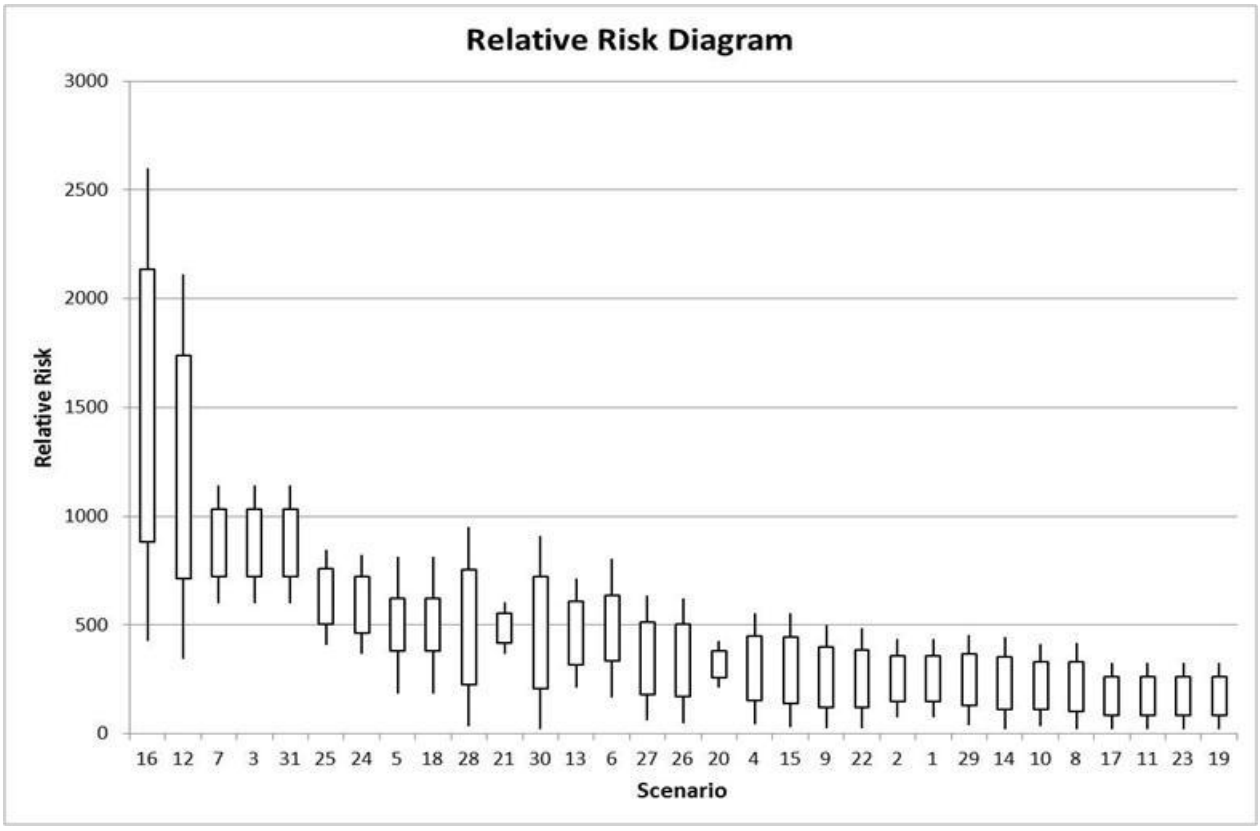

Figure C-6. Relative Risk Diagram with 95 percent Uncertainty Bands

Table C-3. Scales for Assessing Consequences of Disruption

Degree of Potential Effects	Consequence Categories					
	Business Continuity	**Casualty Impact**	**Economic Impact**	**Emergency Response Function**	**National Strategic Importance**	**Replacement Costs**
Catastrophic	Severe degradation or disruption of sector mission fulfillment	Disruption/contamination of supply chain that could result in over 10,000 fatalities	Direct/indirect costs over $100 billion	Severe degradation or disruption of ability of Federal Government to respond at national level	Severe potential for loss of continuity of government or military operations	Replacement cost in excess of $100 billion
High	Significant degradation or disruption of sector mission fulfillment	Disruption/contamination of supply chain that could cause over 1,000 fatalities	Direct/indirect costs over $10 billion	Significant degradation or disruption of ability of federal government to respond at national level	Significant potential for loss of continuity of government or military operations	Replacement cost in excess of $10 billion
Medium	Moderate degradation or disruption of sector mission fulfillment	Disruption/contamination of supply chain that could cause over 100 fatalities	Direct/indirect costs over $1 billion	Significant degradation or disruption of ability to respond at regional level	Moderate potential for loss of continuity of government or military operations	Replacement cost in excess of $1 billion
Low	Minor degradation or disruption of sector mission fulfillment	Disruption/contamination of supply chain that could cause fewer than 100 fatalities	Direct/indirect costs over $100 million	Significant degradation or disruption of ability to respond at local level	Potential for minor but observable effect on continuity of government or military operations.	Replacement cost in excess of $100 million
Negligible	None	Disruption/contamination of supply chain that could cause no fatalities	Direct/indirect costs under $100 million	None	Negligible potential for loss of continuity of government or military operations	Under $100 million

Table C-4. Scenarios Used for Insider Threat Risk Assessment

No.	Sector	Scenario Description
1	Food and Agriculture	Terrorism: An insider contaminates food processing plant via biological attack by introducing toxin into the U.S. milk supply. A 2005 Stanford University study pointed out that the milk industry's distribution systems are vulnerable to bioterrorism through the introduction of botulinum toxin, a deadly poison, into the milk supply. Based on the contamination of a single milk tanker and milk-processing facility, the toxin could be introduced to a large supply of milk via centralized storage and processing. This would dilute the toxin throughout several thousand gallons of milk and lead to widespread consequences.
2	Food and Agriculture	Terrorism: An insider contaminates food processing plant by introducing toxic chemical into the U.S. milk supply. Scenario No. 1 used as proxy for judgments on this scenario No. 2
3	Food and Agriculture	Terrorism: An insider contaminates beef in meat packing plant with E. coli O157 to create loss of confidence in food supply and nation-wide panic.
4	Food and Agriculture	Terrorism: An employee at a foot and mouth disease (FMD) biological-research center in the United States decides to circumvent on-site biosecurity measures to remove live FMD serotype from the facility and introduce it to multiple livestock feedlots and transport nodes in the U.S. "beef belt." This scenario has significant impact on the U.S. beef industry because of the specific serotype; the time elapsed from confirmation of the serotype, the number of animals exposed, and the push for emergency vaccinations.
5	Financial Services	Terrorism, Espionage, Corruption: An insider recruited by a foreign power or criminal organization to conduct cyberattack on an international financial system to disrupt international financial transactions and terrorist financial tracking
6	Financial Services	Terrorism, Corruption: A foreign organized crime group with links to a hostile nation-state coerces a financial clearing house employee, either on the software development or vulnerability management team, to attack the clearing house with the goal of creating massive capital flight from the United States. An insider interfering with time stamps on high-frequency trades could create a sudden liquidity crisis and a potential mini-market crash, thus having a potentially catastrophic impact on the U.S. economy.
7	Commercial Facilities	Terrorism: A disgruntled employee comes under influence of an outside terrorist organization and/or self-radicalizes. The employee learns that he or she will be let go by the company and decides to detonate a Vehicle-Born Improvised Explosive Device (VBIED) against the employer's place of business.
8	Communications	Terrorism: Insiders disrupt supply chain flow of Rare Earth Elements (REEs), which are critical components in cell phones and microwave and satellite communication systems. Insiders instigate political or trade disputes in the country of origin so that that nation purposely reduces or bans exports; or instigate labor strikes that halt the mining and processing of REEs. In 2008 a single foreign country supplied 96 percent of the U.S. imports of REEs; such a disruption in that country could potentially have significant consequences for the Communications Sector.
9	Critical Manufacturing	Terrorism: An insider at a major U.S. maritime port plants a powerful bomb that temporarily closes the port and the effects are felt throughout the CM Sector supply chain. U.S. maritime ports handle two billion tons of domestic and foreign cargo every year. The Critical Manufacturing (CM) Sector, in particular, relies on maritime ports for the import of raw materials, components, and finished products.
10	Dams	Terrorism: A disgruntled employee comes under influence of an outside terrorist organization and/or self-radicalizes. Employee learns he or she is going to be let go by the company and decides to detonate a large Improvised Explosive Device (IED) against a critical point in the dam's facility.
11	Energy	Terrorism: A foreign nation-state recruits an insider sympathetic to the foreign nation to carry out a sophisticated cyberattack on the automated control systems of a U.S. electrical transmission line.

No.	Sector	Scenario Description
12	Energy	Terrorism, Industrial Espionage: A foreign entity recruits an insider to provide essential information to enable them to engineer their hardware and embedded software products so that, once installed, they provide a "back door" for capturing and mapping real-time U.S. SCADA and "smart grid" system data. The information gained could be used to disrupt the system in time of conflict.
13	Government Facilities	Terrorism: A disgruntled employee comes under influence of an outside terrorist organization and/or self-radicalizes. The employee learns that he or she is going to be let go by the government and decides to detonate a VBIED against their employer's place of business.
14	Healthcare and Public Health	Terrorism, Corruption, Espionage: An insider disrupts supply chain flow of critical raw materials for health care equipment. Medical products and services rely on advanced technologies, such as nuclear technologies, that use rare raw materials from only a few suppliers. For example, the global isotope supply chain depends on a small number of aging nuclear reactors for isotope production and a complex processing and distribution chain for delivery of short-lived isotope products to the health care system. A disruption of the supply of the isotope Mo-99 could have significant impact on the global medical supply chain.
15	Healthcare and Public Health	Terrorism: Insider contaminates materials used in pharmaceutical production in an area that has a high concentration of pharmaceutical facilities. This disruption has a devastating effect on the U.S. supply of pharmaceuticals.
16	Healthcare and Public Health	Corruption/Organized Crime: A foreign-based organized crime organization uses insiders to facilitate its Medicare and Medicaid fraud activities in metropolitan centers in at least 20 States. This multinational criminal organization (MCO) is using traditional approaches including creating service providers and sham storefronts, etc. The MCO has recruited or placed insiders in a few major hospitals in the region, in regional Medicare Administrative Contractors, and in Centers for Medicare and Medicaid Services who are involved in claims and billing systems or who can facilitate processing fraudulent claims.
17	Information Technology	Terrorism: A foreign nation-state recruits an insider (with malicious intent after being hired) sympathetic to the foreign nation to attack U.S. electrical transmission lines.
18	Information Technology	Terrorism, Espionage, Corruption: Insider recruited by foreign power or criminal organization to conduct a cyberattack on an international financial system to disrupt international financial transactions and terrorist financial tracking.
19	Chemical and Transportation Systems	Terrorism: A foreign-based criminal organization recruits a criminal alien to detonate a truck containing chlorine inside a tunnel of a major metropolitan area.
20	Energy	Terrorism: A disgruntled employee causes an explosion on an offshore drilling rig in the Gulf of Mexico, resulting in the deaths of several workers, sinking of the drilling unit, an oil spill lasting three months, and various other economic, ecological, and health-related consequences.
21	Transportation Systems	Terrorism: A postal worker who is going to lose his or her job due to cutbacks at U.S. Postal Service (USPS) decides to get even with his employer by introducing an IED into the mail system. The worker has extensive knowledge of USPS air mail handling procedures and is able to circumvent existing countermeasures.
22	Transportation Systems	Terrorism, Corruption: A postal employee is recruited or coerced by an outside terrorist organization to introduce a biological agent into a postal facility. The employee receives financial rewards in exchange for his or her participation.
23	Transportation Systems	Terrorism: An airline pilot going through difficult personal time (e.g., financial troubles, divorce with intense custody battle) decides to deliberately crash the plane into a critical infrastructure asset.

No.	Sector	Scenario Description
24	Transportation Systems	Terrorism, Corruption: A baggage handler is a willing participant in a drug smuggling ring and had previously placed packaged thought to be carrying illegal drugs into the cargo hold of passenger aircraft. Unbeknownst to the baggage handler, the drug smuggling handlers are actually terrorists who eventually swap an explosive or bomb-making components for the "drug package" which then is placed in the cargo hold and detonated, resulting in the catastrophic loss of the aircraft.
25	Transportation Systems	Terrorism, Corruption: An airport screener is a willing participant in a drug smuggling ring and had previously allowed persons carrying drugs to pass through security checkpoints. Unbeknownst to the screener, the drug smuggling handlers are actually terrorists who eventually swap an explosive or bomb making components for the supposed drug package which then is allowed onto a passenger aircraft and results in the catastrophic loss of the aircraft.
26	Transportation Systems	Corruption: For financial gain, a field maintenance worker places an IED on section of pipeline to cause a double shear of pipe in a very remote location.
27	Transportation Systems	Terrorism: A disgruntled railroad employee with access to key bridges (e.g., maintenance worker, or mechanical engineer) deliberately causes mechanical failure at key vulnerable locations on railroad bridges.
28	Transportation Systems	Terrorism: A foreign nation recruits multiple insiders to conduct integrity attacks on rail control centers SCADA/scheduling systems (and other vectors) to delay U.S. military movement.
29	Transportation Systems	Terrorism: A terrorist group recruits an insider to assist with their successful wide-area biological/chemical attack on a major U.S. port. The attack kills or incapacitates the majority of the port's workforce and cripples the port's petrochemical complex and significantly disrupts the petrochemical industry. In addition, the port is closed for an indeterminate length of time, having a severe impact on its economic activity.
30	Border Security	Corruption: A drug cartel near the Southwest border of the United States recruits insiders who have access at border and operating nodes to facilitate expanding influence in United States, in order to gain access to rival group’s territory and financial resources.
31	Water and Wastewater Systems	Terrorism: Terrorist group recruits insiders to inject lethal levels of fluoride into a municipal water treatment plant along the U.S. East Coast to disrupt the drinking water supply and to create panic.

Appendix D: Alternative Futures Development Methodology

Alternative futures serve as an analytic approach informing the findings of the National Risk Estimate (NRE): *Risks to U.S. Critical Infrastructure from Insider Threat*. The alternative futures are not predictions of future events. Instead, they illustrate possible alternatives concerning insider threat and U.S. critical infrastructure sectors, providing lessons and perspectives about insider threat and about these sectors that may help to guide policy and funding decisions.

Alternative futures analysis is used throughout the Government and the private sector to facilitate strategic thinking and planning, enabling analysts and decision makers to identify possible outcomes and alternatives in a structured manner, consider implications of these outcomes, and assess policy options for addressing these potential futures. Alternative futures are plausible alternative views about how the future may develop based on interpretation of observed trends and data; they are *not*, however, predictions or forecasts.[114] Alternative futures analysis enables analysts and decision-makers to consider possible outcomes and alternatives in a structured manner.

The NRE alternative futures were developed based on a methodology that considered a range of key uncertainties for insider threat and the sectors over a 20-year period from 2012 to 2032. The alternative futures development methodology is based in part on a 2008 U.S. National Intelligence Council *Disruptive Civil Technologies* report.[115]

An alternative futures development one-day workshop was conducted in April 2012, resulting in the creation of four alternative future worlds for insider threat across U.S. critical infrastructure sectors. Key strategic uncertainties or major areas that will be of significant importance to the sectors and insider threat in the next 20 years were discussed and weighed on a teleconference before the one-day workshop and further discussed at the workshop. Analysts considered these uncertainties as integral parts of the future of insider threat, and discussed how they might be combined with other factors to create compelling and illustrative alternative futures.

Next, factors were identified that would be valuable in highlighting the challenges to insider threat and the sectors by affecting and balancing the uncertainties. Polarizing perspectives were selected in order to make the alternative futures more distinct. Alternative futures were then built based on the boundaries of the factors and uncertainties.

[114] U.S. National Intelligence Council, *Disruptive Civil Technologies: Six Technologies with Potential Impacts on U.S. Interests Out to 2025*, Conference Report CR 2008-07, April 2008, www.fas.org/irp/nic/disruptive.pdf, accessed March 15, 2012.
[115] U.S. National Intelligence Council, *Disruptive Civil Technologies: Six Technologies with Potential Impacts on U.S. Interests Out to 2025*, Conference Report CR 2008-07, April 2008, www.fas.org/irp/nic/disruptive.pdf, accessed March 15, 2012.

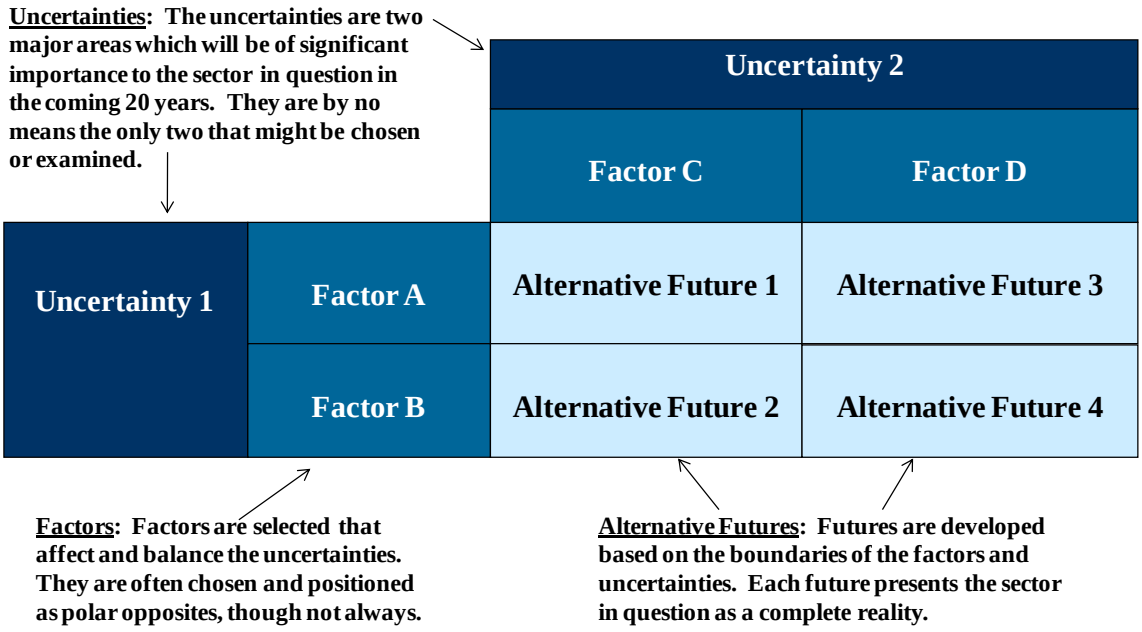

Figure D-1. Developing Alternative Future Scenarios

Two of the four alternative futures were selected as the most critical for further explanation. This decision was based on those alternative futures from which policy-makers might draw the most interesting and valuable conclusions.

The next step in alternative futures workshop is to supplement the four alternative futures concerning insider threat and U.S. critical infrastructure sectors. A small group of Government and private industry subject matter experts developed the alternative futures and accomplished five tasks:

1) Increased the amount of detail and depth for each alternative future;

2) Considered the two primary alternative futures and provided thoughts on the potential challenges and opportunities inherent in these alternative futures;

3) Identified case studies, including projects, innovations, and failures from insider threat and the sectors that illustrate issues captured by the alternative futures;

4) Offered strategic thoughts on the signposts and indicators for the sectors and insider threat to aid policymakers and other customers in determining whether any of the alternative futures are being realized; and

5) Identified the factors that may not have been accounted for in alternative futures development that could bring chaos to the sectors and insider threat.

The results and findings of these discussions are presented in Appendix G.

Appendix E: Tabletop Exercise Methodology

Tabletop Exercises provide a structured analytic approach informing the findings of this NRE. These exercises allow the participants to examine scenarios that are plausible, but do not necessarily reflect existing reality, and do allow the participants to consider both the vulnerabilities of different critical infrastructure sectors to insider attack and the motivations and characteristics of insiders who would maliciously plan to damage U.S. critical infrastructure.

Three Tabletop Exercises

DHS hosted three 1-day exercises during April and May 2012, with each exercise addressing one of three threat themes – Terrorism, Espionage, and Corruption. Each exercise considered three types of insiders – those who have malicious intent before being hired, those who develop malicious intent after being hired, and those who are influenced by outsiders. Each exercise assumed present-day critical infrastructure and policies and involved teams of approximately 20 subject matter experts from the U.S. Government, private sector, and academia with expertise on insider threats, terrorism, homeland security and law enforcement, organized crime, drug cartels, nuclear infrastructure, cybersecurity, and SCADA systems. The teams did not role-play, but rather discussed the issues in a seminar with a facilitator.

- The ***Red Team*** portrayed a variety of insider threats in several attack plans focusing on threats to U.S. critical infrastructure – Terrorism Exercise (five plans), Espionage Exercise (four plans), and Corruption Exercise (four plans).
- The ***Blue Team*** represented U.S. Government interests and developed a response to each of the Red Team's plans by considering vulnerabilities and ways of mitigating the insider threat.

Tabletop Exercise Process and Procedures

Each of the three one-day exercises began with a plenary session, which included background on the NRE and instructions on the mechanics and content for the exercise. The plenary ended with a short scene-setter video for viewing by the participants. All participants then reported to their assigned Team rooms, Red or Blue, and began seminar-style discussions.

During the first hour of each exercise, the Red Team focused on identifying various aspects of its plans while the Blue Team discussed vulnerabilities to infrastructure. After the first hour, the Red Team began developing its first plan and recording the details. The Blue Team continued open discussions during this time. At the close of the hour, the Red Team's first plan was provided to the Blue Team for discussion.

In the following hour, the Blue Team reviewed and developed a response to the Red Team plan. During that time, the Red Team began its next plan. This process continued four or five times, depending on the number of plans each exercise required, and concluded with the Red Team receiving all of the Blue Team's responses. At the end of the day, all SMEs participated in a facilitated plenary hot wash. The Red and Blue Teams discussed their specific plans, decisionmaking processes, and broad ways to mitigate the insider threat.

Post-Exercise Evaluation and Analysis

Notetakers captured the discussions in each Team room, the results of plenary discussions, and the plenary hot wash. The NRE team then analyzed data from these exercises and documented the analysis and results for use in the NRE chapters and appendices.

Appendix F: Insider Tabletop Exercise Key Themes

DHS hosted a series of Red-Team-Blue Team tabletop exercises to elicit subject matter expert judgment on various attack scenarios involving three types of insider threat to U.S. critical infrastructure: Terrorism (April 20, 2012), Espionage (April 25, 2012), and Corruption (May 1, 2012). Throughout the exercises and post-scenario discussions, the subject matter experts examined insider motivations, tactics, and decision-making and provided insights regarding likelihood, consequences, vulnerabilities and risk mitigation measures related to the insider threat. The latter included discussions on relevant best management practices or identified gaps and weaknesses in existing Prevent, Protect, Mitigate, Respond, Recover (PPMRR) measures. (See Appendix I for a list of subject matter expert participants.)

Summary of Key Themes

Defining Success from the Insider's Perspective

The terrorist insider's intent is to use his or her access/knowledge to perpetrate an attack against a strategic or political opponent that discredits the industry, erodes confidence in the U.S. Government, and causes mass fear and distrust. Regardless of the effectiveness of current safeguards in preventing attacks, the terrorist insider may have multi-layered and nuanced ways of defining "success." Simply being able to prove or claim to have found chinks in the U.S. critical infrastructure security armor may be enough to have a debilitating psychological impact. The challenge then becomes how well the sector and the U.S. Government are prepared to assuage fears and deal with potential hysteria whether or not an actual attack occurs.

Supply Chain Vulnerabilities

Even with seemingly solid insider prevention and mitigation programs in place, there is always room for improvement, especially as they do or do not address third-party insiders (vendors and contractors) and critical elements of the cyber supply chain that are less likely to embrace the same culture of security. High personnel turnover rates throughout project or contract phases combined with an ability to carry out work with relatively low levels of oversight and high degrees of anonymity increases the risk of third-party employees becoming "virtual insiders." In addition, the lack of oversight and rigorous, enforceable standards for software development, manufacturing and validation are major concerns for many industries and sectors, particularly with the gradual migration from analog to digital control systems.

The subject matter experts voiced concern that the software validation process for most critical infrastructures may not be consistent or thorough enough to detect a malicious code attack executed with a high-level of sophistication, and then only thorough enough through code review in the software lifecycle, if implemented properly. They also doubted whether a software test would detect a cyber "time bomb." Further, the subject matter experts stated that there is no rigorous software manufacturing industry control process in place. They generally agreed that the best way to prevent this type of cyberattack from occurring is to require software engineering discipline as rigorous as that found in the airline industry, for example. The subject matter experts also agreed, however, that the transition to Maturity Level 5[116] software development

[116] Capability Maturity Model Integration (CMMI) in software engineering and organizational development is an approach that provides organizations with the essential elements of effective process improvement. CMMI Level 5

protocols would take years. The team felt that requiring independent, third-party software reviews also will require significant investments of time and money that software and utility companies cannot justify based upon the limited threat level they perceive.

Attractiveness of SCADA and ICS as Targets

Neither the U.S. Government nor the private sector is aware of the full scope of cyber vulnerabilities within the array of the Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) that monitor and control equipment and processes in industrial and manufacturing facilities and in major critical infrastructures such as the North American electrical grid and municipal water purification and distribution systems. Most current SCADA systems were not designed with the threat of espionage, data exfiltration, malicious intrusion, and insider threats in mind. As a result, cybersecurity concerns still are often eclipsed by operators' overriding focus on operational safety, productivity and efficiency – what the subject matter experts characterized as an "engineer's mindset." In the absence of universally accepted and enforced cybersecurity standards, to include the identification of critical facilities and systems, the trend toward more open, interconnected, Web-based industrial control systems leaves them increasingly vulnerable to undetected reconnaissance, mapping, and attack.

The subject matter experts also noted that although almost all utilities use SCADA, many of their communications functions are wireless and use inexpensive, non-secure two-way radios. Depending upon the utility, system manipulation could be as easy as having an individual, equipped with radio gear and a properly configured laptop and sitting in a nearby building, who conducts remote override attacks via radio signals sent to a control device without authentication. To illustrate this point, one subject matter expert highlighted the 2000 Vitek Boden cyberattack against a sewage pumping station in Australia.

Back-Up Systems as Secondary Targets

In SCADA and non-SCADA environments, the subject matter experts acknowledged the advantage that malicious insiders and foreign adversaries could gain by including back-up command and control systems and software in their cyberattack plans in addition to the primary target to hinder response and recovery. This includes targeting continuity of operations plans as sources of information to inform an attack. To create catastrophic consequences, the insiders must include these systems into their overall attack plans. For example, one subject matter expert noted that a typical electric power transmission or pipeline system backup site can be made operational in a reasonably short time frame that prevents serious consequences.

Technology and the "Virtual" Insider

Technology increasingly is blurring the line between the physical and the "virtual" insider determined to conduct espionage and sabotage. As such, the subject matter experts agreed that many aspects of the espionage attack scenarios could just as easily have been accomplished by a persistent, knowledgeable individual using a laptop. Related to this is the problem of preventing and mitigating supply chain sabotage by third-party vendors and subcontractors of software or control systems who have remote access credentials and maintenance privileges for critical

---

focuses on optimizing process improvement. See Carnegie Mellon-Software Engineering Institute, Capability Maturity Model Integration (CMMI), www.sei.cmu.edu/cmmi/, accessed July 19, 2012.

infrastructures associated assets. Subject matter expert discussions on access also included concerns that security measures should adequately deal with preventing access to as well as the *extraction* of data.

The subject matter experts offered one aspect of a "virtual insider" scenario in which a foreign terrorist group co-opts a disgruntled SCADA vendor into providing them with existing remote access authority and knowledge of a utility's credentials and hardware/software configurations. As a result, the terrorists gain a remote pathway into the utility via the supply chain and become new "virtual insiders" who are able to alter data within the SCADA/human machine interface (HMI) system such that normal functions do not occur or do occur but in a different way.

- Several subject matter experts noted that performing security controls to a certain specific standard across industries would have a significant mitigating effect on such scenarios, particularly as they pertain to credentialing, configuration management, system logs and monitoring, and patching. One subject matter expert cited the evolving NERC standards as a good starting point but noted that even these standards require further analysis to discover weaknesses in the system. He also offered that advanced/integrated configuration management already is in use with larger control systems.
- The subject matter experts agreed that smaller municipally regulated companies are likely to have limited resources and awareness to deal adequately with mitigating insider threats of this nature. They also agreed that restrictions and complex privacy constraints hinder information sharing between the U.S. Government and the private sector. Exacerbating the problem is that fact that many of these infrastructures lack a central corporate headquarters with which the U.S. Government could interact.

Identifying Critical Assets within Critical Infrastructures

The subject matter experts stressed the need to identify systemically critical infrastructures and assets within critical infrastructures to harden them against becoming single points of failure. Hardening measures would include not only physical security measures but also fully integrated cybersecurity and human resources protocols to ensure that no high-risk behaviors or activities fall through the cracks. Both teams agreed that employees of designated critical infrastructures and assets should be held to a high standard and that private entities should have the appropriate mechanisms to request and receive background and watch lists for prospective employees who may be high risk.

A considerable amount of subject matter expert discussion focused on the need for sound hiring practices that include comprehensive background checks, periodic follow-up investigations, and identification of behavioral "red flags" among members of the existing workforce. The question was raised regarding whose responsibility it would be to investigate individuals in an increasingly multicultural workforce who, by virtue of emotional, familial, or business ties to their countries of origin or to a more global community, may be subject to foreign influence or motivated to conduct espionage or sabotage on behalf of a foreign nation-state or cross-border/transnational criminal entity. Such indicators would fall outside the scope of routine criminal history checks and, even if detected, would pit the corporate culture and legal concerns in the private sector against counterintelligence concerns and perceived concerns in the U.S. Government sphere. The subject matter experts envisioned a "nightmare scenario" in which an insider with ethnic ties and an affinity for a foreign nation-state conducts espionage that lays the groundwork for a contingency attack against U.S. critical infrastructure. The major concern

among the subject matter experts was how the U.S. Government would mitigate and respond to such an event in light of political sensitivities and ill-defined "red lines" as to what constitutes an act of war in the cyber realm.

The Need for "Big Mosaic" Thinking to Recognize Threat Patterns across Sectors and Public-Private Jurisdictions

The subject matter experts generally agreed that considerable work remains to be done in terms of analyzing an overwhelming body of data and centralizing reporting on global cyber incidents across critical infrastructure sectors and public and private jurisdictions in order to recognize patterns. This includes revisiting fused or joint intelligence methodologies that foster law enforcement and private participation. The group acknowledged that there is considerable insider threat and cyber reporting that does not escalate to the point of influencing policy, noting that this step is difficult if no one dies or sustains physical injuries from a cyber-related incident. Desensitization to small-scale malicious acts over long periods of time increases the cyber and human intelligence challenge of being able to recognize a network of problems as part of a single nefarious plan. In addition, the group asserted that there is a difference between espionage and attacks against systems in terms of how they are treated and reported. The subject matter experts noted that no single entity is responsible for the difficult task of synthesizing seemingly disparate data and articulating what they all mean. Even if such an entity did exist, the group questioned where the fused reporting would go and by what mechanism(s). The subject matter experts concluded that problems of this scale and complexity require a long-term national vision, which perhaps only a "Cyber 9/11" or similar catastrophic event can instigate by forcing the government and private sectors to change their disjointed approach to cyber espionage.

Most subject matter experts considered the difference in corporate cultures between the government and private sectors to be a major stumbling block in terms of how they approach the issue of security, noting that the private sector's perception of government levying of invasive and proscriptive vetting, hiring, and network and behavioral monitoring policies may be a perpetual source of friction. The challenge rests in bringing the two parties together, particularly when the protection of critical infrastructure and associates systems is concerned. There was brief discussion that the process of migrating private infrastructures from using minimum, cost-effective standards toward implementing best practices and employing right-minded thinking might involve a combination of regulation and market incentives to do so.

Define and Enforce Cyber "Red Lines"

Related to their concerns about the lack of "big picture" analysis on cyber espionage, the subject matter experts also discussed the issue of outlining indicators for communicating and enforcing "red lines" for cyber incidents that clearly define tripwires and operational responses (rules of engagement) at all levels, both public and private. They considered the problem particularly acute in the event of an espionage/intelligence preparation of the battlespace scenario that plays out under the radar for an extended period of time. They characterized the problem as "cybersecurity being popular until it is time to do something about it." In the absence of legal, agreed-upon response thresholds, the "red lines" keep moving and are ill-defined. As a result, it is unclear as to when, how, and at what levels the United States would respond to various types of cyberattacks. As in the case of a "zero-day" exploit that lies dormant for an extended period of time, what activity indicators should be identified from the clutter? Waiting until there is visible, physical damage may be too late. Within the larger context of nation-state espionage,

especially with respect to countries over which government and business objectives or corporate cultures are at odds, at what point do cyberattacks constitute an act of war versus a mere disruption? The subject matter experts asserted that sophisticated adversaries will know how to use legal, institutional, and cultural constraints in the United States to their advantage to buy time against any response.

Insider Threat Programs

The subject matter experts overwhelmingly identified robust insider threat programs as the key to identifying insider threats based on corruption. The subject matter experts acknowledged that programs exist but explored how they could be more effective. The key to creating an effective program is identifying particularly vulnerable positions and training individuals who fill them on effective security protocols. The subject matter experts also voiced the need for continuous monitoring and creation of a "culture of integrity" wherein employees are incentivized and provided mechanisms to report observable changes in workplace behavior and other anomalies. This would alert officials when an employee might be compromised or is at higher risk of being compromised.

The subject matter experts agreed that an effective critical infrastructure insider threat program must, at a minimum, include vulnerability checks, integrity testing, background checks for all family members of employees, regular behavioral monitoring and vetting, and periodic polygraph testing. There was some discussion of randomizing work type and shifts; however, some subject matter experts thought this could be demoralizing for the entire workforce. They also discussed instituting positive incentive programs for employees to report suspected corruption or questionable behavior within the workplace. The subject matter experts considered training and awareness crucial so that each member of the target population understands his or her vulnerability for recruitment. Any and all of these measures along with a strong counterintelligence capability, intelligence sharing protocols, and effective employee reporting mechanisms could form the backbone of a solid insider threat program. In addition, the some subject matter experts noted that mutual information sharing agreements with foreign governments play a significant role in helping detect and prevent all types of illicit cross-border activity unless, of course, the foreign intelligence counterparts are themselves complicit in illegal activities.

The subject matter experts asserted that the greatest stumbling block to creating more robust insider threat programs is funding. As an example, they noted that border entry ports (and associated critical infrastructure) typically are joint public-private enterprises. In this context, the private sector would be unlikely to invest in costly insider threat programs and access control systems in the absence of an actual or perceived threat. Institutional resources may not allow for increased analytics and private entities may not be able to justify investment in what are perceived as low risk areas.

Exploitation versus Attack

The notion of an attack on critical infrastructure is a fluid concept, particularly for organized criminal gangs. Border corruption is a current reality; however, an attack on critical infrastructure involving the co-option of insiders is more often focused on exploiting and working within the system to achieve organizational ends rather than by simply destroying critical nodes for ideological and symbolic purposes. This represents a significantly different

mindset from that of a terrorist insider and should be taken into account when corruption is a suspected motivation for an attack.

- In discussing a hypothetical transnational organized crime attack using co-opted insiders to install malware and botnets on computer systems of various financial institutions, the subject matter experts identified several countermeasures that the banking and finance industry currently has in place that could potentially deter or recognize such an attack. Banks should have reporting requirements in place for account manipulations and subject matter experts agreed that strong IT access controls and strong network controls could help defend against the insiders perpetrating the attacks. Further, normal auditing and monitoring may begin to detect the pattern of the attack over time. Detection software for large transfers and extractions is already in place in most banking institutions and subject matter experts considered that this could be extended to small scale extractions over time to help determine the insiders perpetrating the attack. Further, the introduction of IT protections that would make each transaction traceable or improved industry software standards could improve significantly the ability of the industry to combat this attack.

The Public-Private Nature of Infrastructure

The subject matter experts repeatedly indicated that the public-private nature of the owners and operators associated with U.S. critical infrastructure means that insiders are able to circumvent any action taken by the U.S. Government to prevent corruption if private contracting companies do not have similar safeguards in place. Private companies control many border crossing points, such as bridges and tunnels, and support other critical U.S. Government functions through contractors. These companies have no economic incentive to place restrictions on their employees or to institute potentially cost-prohibitive insider threat programs without a clear and present threat or a government mandate. As such, information sharing with the private sector is vital to securing U.S. critical infrastructure from attacks precipitated by corruption.

In terms of reporting security breaches to U.S. Government or intelligence agencies, the subject matter experts considered that there is a general reticence of private industry, particularly in the banking and finance arena, to do so. They did point out, however, that various agencies allow anonymous reporting of security breaches.

- Subject matter experts briefly discussed the extensive number of private and public intelligence gathering institutions involved in intelligence sharing and investigation of electronic crimes in the Banking and Finance Sector. The Financial Services Information Sharing and Analysis Center (FS-ISAC) is particularly important as a private sector organization that allows banks to report breaches and thefts anonymously. The FS-ISAC actively collaborates with the Department of Homeland Security and shares information with the Financial Crimes Enforcement Network (FINCEN) at the U.S. Department of Treasury and the Electronic Crimes Task Force (ECTF) at the U.S. Secret Service. The subject matter experts agreed that information sharing between the banks and these organizations would be necessary and helpful to recognize the attack and the insiders perpetrating the attack.

- Attacks with an international nexus present a problem for information sharing. The Financial Action Task Force (FATF) is an intergovernmental agency designed to facilitate global conversation on money laundering, terrorism, and other international financial crimes. However, some countries are reluctant to share information or engage with FATF. Institutionally, an attack on banking and finance has unique constraints. Subject matter experts agreed that if insiders are high-level executives, they may be given broad access to systems and proceed without their actions being questioned. Further, banks have to maintain standards of personal privacy, protect their proprietary software, and have a tradition of not disclosing problems that could increase the severity of the attack.

Types of Insiders

The subject matter experts considered the actions of three different types of insiders (an insider who had developed malicious intent before being hired, an insider who developed malicious intent after being hired, and an insider who was influenced by outsiders to use his or her access to carry out an attack). While there were differences in motivations among the three types, they did not significantly affect the attack responses. The one distinct difference noted was that robust initial personnel screenings could help identify an insider who had developed malicious intent before being hired.

- There was general agreement that the insider who is extorted or otherwise influenced by an outsider is much more difficult to identify than an insider who had malicious intent before being hired and would have to process through personnel security before beginning employment.

Appendix G: Insider Alternative Futures Workshop Findings

Introduction

DHS hosted a one-day workshop on April 3, 2012 to elicit subject matter expert judgment on alternative futures that could present challenges and opportunities related to malicious insider threats to U.S. critical infrastructure over the next 20 years. The alternative futures discussed are not intended to predict the future but to examine plausible combinations of uncertainties and contributing factors that tell a series of compelling stories about how the nature and mitigation of the insider threat could evolve if each specific future became a reality. The workshop participants also discussed potential signposts and indicators that might correspond to each alternative future, as well as strategic surprises that could significantly alter their trajectories. (See Appendix I for a list of the NRE Alternative Futures Workshop participants.)

Analytic Assumptions

Workshop participants based their alternative futures analysis on the following assumptions, which are intended to be viable for the 20-year outlook period of this NRE:

- There will continue to be insider threat risks to U.S. critical infrastructure.
- Malicious insiders will be more technologically savvy and increasingly capable of defeating security countermeasures that are static, improperly scoped, or unable to keep pace with the evolving threat.
- The line between internal and external threats will be increasingly blurred because of the proliferation of digital, Web-based technology within business and control systems.
- Major investments in U.S. critical infrastructure to mitigate insider threats will not be universal or consistent.
- Innovation and/or effective risk management will be able to mitigate certain aspects of insider threat risk.

Key Themes

The workshop discussion yielded the following key judgments regarding potential future landscapes for the insider threat to U.S. critical infrastructure over the next 20 years:

- Traditional "low tech" malicious insider techniques remain viable, even in a technologically advanced future, because adversaries will continue to adapt to exploit vulnerabilities and gaps in the prevailing security environment.
- Migration to dependence on the "cloud" environment provides insiders significantly increased opportunities to execute systemic and repeatable attacks that could affect all critical infrastructure sectors and exploit their virtual supply chain vulnerabilities, particularly with regard to the feasibility of both hypervisor and inter-virtual machine (VM) attacks.[117]

[117] The hypervisor, also called a virtual machine (VM) manager, serves as the control panel ("brain") of the virtualized "cloud" infrastructure, allowing multiple operating systems (OS) to share a single hardware host. The

- The trend toward blended (cyber and physical) attacks against critical infrastructure will force the issue of a convergence between the cybersecurity and physical security organizations to foster a more holistic approach to managing risk against a much more sophisticated and broad spectrum insider threat.
- Globalization and outsourcing as they relate to U.S. critical infrastructure will increase current challenges associated with employee privacy and trust issues in any alternative future environment.

Overview of Alternative Futures Uncertainties

The workshop participants selected **governance** and the **insider capabilities** as two major uncertainties that will drive the alternative futures related to the insider risk to the 16 U.S critical infrastructure sectors. Figure G-1 outlines the four alternative futures identified for this NRE that are based upon these two uncertainties and their associated factors.

		Insider Capabilities	
		Traditional Techniques	**Technology Enhances**
Governance	**Haphazard**	**Tried and True Will Do**	**Mission Impossible**
	Effective	**Advantage Good Guys**	**Cold War**

Figure G-1. Insider Threat Alternative Future Matrix

Governance

For the purposes of this NRE, the subject matter experts adopted a performance-based risk management approach to governance as it relates to creating an organizational framework to counter the evolving insider threat that includes:

- Clearly defined insider threat program policies and procedures;
- Expectations for consistent training, compliance, and policy enforcement that are scalable across organizations and critical infrastructure sectors;

---

hypervisor is a layer of abstraction between VMs and the underlying hardware, allowing for the dynamic allocation of system resources. Although each OS appears to have the host's processor, memory, and other resources all to itself, the hypervisor actually controls the host processor and resources, allocating what is necessary to each OS and ensuring that the VMs do not disrupt one another. If the hypervisor is compromised, then the entire infrastructure can be controlled and infected at once. Inter-VM attacks involve individual virtual machines attacking other virtual machines. This is problematic because most cybersecurity technologies have no visibility into what occurs within virtual machines. See *Changing the Game for Anti-Virus in the Virtual Datacenter*, Trend Micro White Paper, September 2012: 2, and http://searchvirtualization.techtarget.com/definition/virtual-machine. For further discussion on hypervisors and VMs, see also Mitchell, Robert L., "Hypervisor as virtualization's enforcer?," August 10, 2010, http://www.computerworld.com/s/article/9179910/Hypervisor_as_virtualization_s_enforcer_

- Appropriate parameters for employee screening and behavioral monitoring that take into account legal and privacy considerations as well as potentially negative impacts on operations, productivity, and morale;
- Robust cooperation and coordination between those responsible for the cyber and physical security aspects of the insider security program; and
- An end goal of safety and soundness through governance, which is about protecting critical infrastructure assets and insulating them from risk.

The workshop participants unanimously agreed that risk management is a function of good governance. After that, it becomes a question for leadership to determine how best to execute it. The subject matter experts also discussed their perception that the United States lacks an overarching industrial policy standard regarding insider threats to critical infrastructure, referring to this as one of our Nation's greatest weaknesses. While regulations exist in certain sectors and industries, others demonstrate a significant lack of visibility on the insider threat. Even where insider threat policies and programs are in place, execution, enforcement, and verification may be inconsistent. In addition, not all of these policies and programs necessarily address the many nuances of the evolving insider threat that cross personnel, physical, and cybersecurity domains. Several subject matter experts voiced concern that effective policies in the future *must* address a stakeholder's ability to identify, monitor, and deal with at-risk employees. WikiLeaks and similar cases were cited as making the case that policy alone – just like improved technology – is insufficient in dealing with the full range of insider threats.

A recurring theme throughout the governance factor discussion was concern about the traditionally bifurcated cyber and physical security worlds and the need for governance to make the two fiefdoms work together in securing critical assets against the insider threat. The workshop participants posed the following questions. Is it the Chief Information Security Officer (CISO) who implements policies to preserve the integrity of access controls or the Chief Security Officer (CSO), who is more technical? At what point does organizational governance change to deal with this duality of responsibilities? The subject matter experts had no specific answers to the questions but did agree that the end goal should be CISO-CSO collaboration supported by governance and funding to make it a reality.

Insider Capabilities

Based upon several of the key assumptions that address current threat data and trends, the workshop participants agreed that juxtaposing malicious insider capabilities with varying states of governance affecting insider risk management provided the most compelling range of alternative futures scenarios for discussion. Within the context of this NRE, capabilities refer to the diverse and evolving suite of tactics, techniques, and procedures available to the malicious insider, who continually is forced to make trade-offs in terms of how and when they can be leveraged most effectively against the existing security environment. Of particular interest to the group was the premise that most insider threats today are facilitated by cyber and that the problem only becomes worse as we increase trust in the "cloud," which currently is not considered critical infrastructure for the purposes of risk management.

Alternative Futures Discussions

The alternative futures were designed to highlight challenges for U.S. critical infrastructure stakeholders that can be extrapolated from available data on current insider activities and trends.

This section draws from discussions by workshop participants to provide a more detailed narrative description of the insider threat environments that characterize the four alternative futures scenarios depicted in Figure H-1. In addition, this section includes assessments on potential challenges and opportunities as well as signposts and indicators for two scenarios selected by the subject matter experts for more in-depth examination and discussion (Advantage Good Guys and Mission Impossible).

Tried and True Will Do

In the Tried and True Will Do alternative future, haphazard governance creates a permissive, target-rich operational environment for even the least technologically savvy malicious insider, somewhat analogous to the current state of affairs. The insider is able to press the advantage in a world characterized by inconsistent, *ad hoc*, or non-existent policy implementation as well as a relatively high level of insider risk tolerance. Insiders continue to use the most expedient and effective methods to target what they perceive as the easiest to access, i.e., opportunistic attacks against the "low-hanging fruit." Because the majority of insider attacks in this future tend to be relatively "low tech" and localized, as a function of the perpetrator's level of physical or cyber access, existing physical protections systems may be able to prevent some attacks.

Overall, the workshop participants thought that this scenario reflects how the status quo regarding prevention of and protection against the insider threat only becomes worse. Even in 20 years, the more traditional, physically based, "low-tech" insider techniques, tactics and procedures remain viable if the perpetrators are able to execute "A- to B+ types of attacks because there continues to be only B- protection in place." The insider in the Tried and True Will Do world could and likely will employ more sophisticated tactics but is not required to do so to be effective.

Workshop participants noted that the majority of insider espionage events involve traditional, physically-based attacks, i.e., by virtue of their jobs the insiders simply need access to the information or asset they are targeting. They pointed to WikiLeaks and the Defense Intelligence Agency/Ana Montes espionage case as examples of insiders who did not use technologically advanced techniques to exfiltrate data. Even with policies in place, these individuals had a reasonably good understanding of what they could do without sending up "red flags." The subject matter experts also noted anecdotally that in the financial sector one could make withdrawals up to $3,000 without attracting undue attention. CMU-SEI CERT's insider database includes cases in which janitors were able to steal items marked "trade secret" or which contained personally identifiable information (PII).

The severity of insider attack consequences in the Tried and True Will Do future varies widely. Within the context of risk tolerance priorities and increasingly disproportionate focus on cybersecurity, the workshop participants emphasized that even a relatively "low-tech" traditional attack executed well can be as potentially high-impact as a technologically sophisticated attack. The major difference is that the traditional insider may require a longer planning and execution cycle and, consequently, face a higher risk of exposure. He or she may only succeed in exfiltrating one piece of paper, but that one piece of paper in the wrong hands could be disastrous

for national or organizational security.[118] Participants asked what procedures are in place to deal with the malicious insider who simply memorizes sensitive information and walks out the door.

Longer timelines and the more localized nature of insider threats in this alternative future afford critical infrastructure stakeholders some opportunities for recourse because the organization has the ability to affect the insiders well-being in an environment where he or she may not enjoy the degree of anonymity that a sophisticated "digital insider" would.

Cold War

In the Cold War alternative future, only the most sophisticated, technologically savvy, and resourceful insider or groups of insiders will succeed. As discussed in the Advantage Good Guys future, the insider has to work harder to identify and penetrate facilities, systems, and assets that are *not* protected. Effective governance reduces the risk to U.S. critical infrastructure through fully integrated physical and cybersecurity management practices that include legal mechanisms to collect, monitor, share, and operationalize relevant insider threat data and behavioral analysis, even against mobile devices and social media. The irony is that insiders in this future may be forced to resort to more traditional tradecraft and TTPs, at least in the short term, if governance is effective and agile in keeping pace with the full spectrum of advanced insider threats.

The workshop subject matter experts assessed that insider success in this world most likely would have widespread and disastrous effects. They also agreed that a highly effective insider threat program must incorporate behavioral analysis tools and technical solutions that potentially are automated.

Integrated and adaptable physical and cybersecurity risk management programs are critical to managing the sophisticated insider threat, particularly in a future where adversaries may be forced into collusion with other insiders and outsiders to succeed.

Policies and governance that support the ability to monitor and collect more relevant insider data, such as information off mobile devices and social media, could help detect the insider but would require a delicate balance between personal privacy issues and national security requirements as they pertain to U.S. critical infrastructure in the United States and abroad.

[118] According to a 2011 CMU-SEI CERT insider threat blog, 36 of over 500 cases in the CERT insider threat database involved the exfiltration of sensitive data using printouts or devices that allow the extraction of digital information to paper or the management of paper documents, such as printers, scanners, copiers, and FAX machines. The report asserts that these types of devices often are overlooked in enterprise risk assessments. See CERT Insider Threat Team, "Data Exfiltration and Output Devices - An Overlooked Threat," October 17, 2011, www.cert.org/blogs/insider_threat/2011/10/data_exfiltration_and_output_devices_-_an_overlooked_threat.html , accessed September 6, 2012.

Advantage Good Guys

In the Advantage Good Guys alternative future, the traditional insider must work harder and risk exposure to identify and target what is *not* guarded in his or her domain to be successful. Effective governance (as it applies to U.S.-based versus overseas operations) creates a higher probability of detection, greatly reducing the overall risk of an insider attack. In this world, insider collusion may become more of an imperative to overcome layered defenses with more physical and cyber threat mitigation controls in place. Even collusion may not be enough to defeat more robust insider threat detection programs that incorporate advanced and potentially automated behavioral analysis tools.

Workshop participants stated that a higher risk of exposure and detection as well as the relative localization of the threat make successful insider attacks less likely. Effective and integrated physical and cybersecurity policies will make it more difficult for insiders to act alone. Even collusion would demand the expertise of technical and non-technical insiders to overcome the enforced countermeasures.

As in the Cold War future, the workshop participants agreed that that a highly effective insider threat program must incorporate behavioral analysis tools and technical solutions that potentially are automated. In addition, both public and private organizations will need to assess the best security procedures that also respect employee privacy, a trade-off that will test effective governance in the face of advances in the digital world. Also similar to the Cold War future, insiders in the Advantage Good Guys world may be forced to resort to more traditional tradecraft and methods, at least in the short term, to circumvent effective countermeasures if governance is effective and agile enough to keeping pace with or get ahead of the full spectrum of advanced insider threats. The workshop participants envisioned that the Advantage Good Guys and Cold War alternative futures go back and forth as each side flexes to gain the advantage. In both worlds more insider activity may be detected and prevented, but the "arms race" continues.

Challenges

The workshop participants outlined the following challenges for public and private critical infrastructure stakeholders in the Advantage Good Guys alternative future.

- Avoiding the tendency of stakeholders to rest on their successes by maintaining and continually evaluating effective governance in the face of constantly evolving threats;
- Striking a balance between operational efficiency/mission accomplishment and implementing comprehensive, effective insider threat security programs;
- Managing and distilling potentially enormous amounts of data from multiple sources, e.g., social media, physical detection systems, cyber, behavioral profiles, etc., into actionable information;
- Retaining adequate funding for governance;
- Maintaining situational awareness of the degree of "consumerization" of the insider threat in terms of the number and destructive potential of traditional, "low-tech" tools available on the open market and via the Web;

- Treating globalization of the workforce as a delicate balancing act between exploiting new business opportunities and efficiencies while not giving away our security strategies; and
- Maintaining employee trust in an increasingly globalized world.

Opportunities

The workshop participants outlined the following opportunities for public and private critical infrastructure stakeholders in the Advantage Good Guys alternative future.

- Establishing and sharing best practices that are accepted by overseas partners. The workshop participants generally agreed that the United States has not yet been successful in mitigating the global threat to U.S. critical infrastructure. Even if the United States becomes a less vulnerable target in the Advantage Good Guys scenario, the same cannot be said for overseas enterprises and operations that affect U.S. critical infrastructure and its supporting supply chain;
- Potentially lowering costs, primarily legal and insurance-related, because of the reduced or contained insider threat; and
- Establishing and improving employee insider threat awareness training.

Signposts and Indicators

The workshop participants identified the following indicators that can signal public and private critical infrastructure stakeholders that the Advantage Good Guys future may be emerging.

- Development and implementation of effective policies that include dialogue, public-private information sharing, standards, performance metrics, and deliverables;
- Adoption of employee privacy laws that specifically address the many facets of mitigating insider threats to physical and cyber assets (primary and supporting) that are deemed as U.S. critical infrastructure;
- Reduction in the number of insider attacks (successful and unsuccessful). One facet of this includes successful containment of attacks before the worst happens;
- Emergence of a "human firewall" through increased awareness, employee training, and well-crafted reporting programs for insider indicators, e.g., behavior, financial, travel, contact, stressors, etc. This includes employees knowing the mechanisms through which they can report such information. The subject matter experts emphasized that increased reporting does not necessarily mean that the insider problem is getting worse but may simply reflect an increased awareness of it. This becomes a critical complement to advanced cyber, technical, and physical security programs;
- Availability of effective insider threat risk-based prevention and detection technology that correlates disparate data sources to potential technical and behavioral indicators of malicious activity while adhering to employee privacy laws;
- Implementation of standardized personnel policies that inform stakeholders what to look for and how during pre-employment screening and employee monitoring. This goes well beyond background and criminal checks; and

- Reinforcement of high-quality, dynamic, formalized education and training on insider threats that is reinforced at all levels of an enterprise. This includes offering college-level courses for risk managers.

Mission Impossible

In the Mission Impossible alternative future, the insider is more capable and diverse than ever before, making effective risk management extremely difficult, if not impossible. A haphazard culture of governance sets the scene for repeatable and systemic insider attacks. In this world, an increased number of insiders using technologically enhanced techniques can launch targeted and potentially widespread attacks with impunity from one or multiple vectors with minimal risk of attribution. Outsourcing continually broadens the field of potential adversaries in the U.S. critical infrastructure virtual supply chain. The truly "high-tech" insiders have a significantly enhanced asymmetric capability to create widespread kinetic impact though cyber means. Perhaps more highly destructive is their ability to conduct widespread cyber exploitation attacks, the effects of which cannot be readily seen before resulting in potentially catastrophic consequences. The workshop participants agreed that the sophisticated insider actors in this world become systemic threats because they will happily come back for more until someone is able to stop them. In essence, most technologically advanced adversaries do not want to disrupt services that might support their overall strategy.
Cybersecurity may prevent or detect some attacks, but strategic response is limited because an attack may go undetected and is unlikely to be localized or easily attributable in this future world. Physical protection systems may be compromised more easily because they, too, are IP-connected. The workshop participants agreed that even effective governance would be unable to counter the technology-enhanced insider. A professional 20 years from now will know how to obfuscate and cloak identities in a haphazard governance environment.[119]

Workshop participants discussed three major factors that will drive the non-localized nature of the malicious insider threat in the Mission Impossible future: 1) increased use and dependence upon the "cloud," 2) an increasing trend toward outsourcing to address business inefficiencies and market demands, and 3) the role of technology in increasing the "converged threat" (cyber and physical) against U.S. critical infrastructure.

The "Cloud." Most insider threats today are facilitated by the cyber domain, and it is not always the user that is compromised, but sometimes the device used. The "cloud" has expanded the boundaries of critical infrastructure, much as it has the scope and reach of the "digital insider," without being treated and protected as critical infrastructure in itself. Trust in the "cloud" increases risk because of increased opportunities for remote access to critical systems. The workshop participants agreed that malicious "cloud" use scenarios are frightening because potential impacts go well beyond the cyber realm, for example, if the "cloud" is exploited to initiate radiological or biological attacks. There will be numerous technological advances that

[119] According to the U.S. Government Accountability Office, the number of cybersecurity incidents reported by Federal agencies to US-CERT increased approximately 680 percent between Fiscal Year 2006 and Fiscal Year 2011. US-CERT does attribute the increase, in part, to agencies improving their detection and reporting of network security incidents. See U.S. Government Accountability Office, *Cybersecurity: Threats Impacting the Nation,* GAO-12-666T, April 24, 2012: 9, www.gao.gov/assets/600/590367.pdf, accessed September 6, 2012.

will affect U.S. critical infrastructure over the next 20 years whose potential security vulnerabilities will need to be evaluated before fielding on a wide scale. Unfortunately, technology moves quickly and malicious actors will be the first to leverage it to suit the needs.

Outsourcing. Going hand-in-hand with concerns over the "cloud" and the ambiguity of insider threat boundaries are the issues of outsourcing and virtual supply chain threats, common themes raised throughout the alternative futures workshop and tabletop exercises for this NRE. Having both classified and otherwise sensitive information in the "cloud" creates a group of new insiders (subcontractors) with access and the ability to manipulate or give away information no longer stored at home base. With inefficiencies and the market place forcing more third-party outsourcing, organizational IT departments will be the first to be downsized and with them localized control of how to identify and mitigate insider threats will be reduced.

The "Converged Threat." Advances in information technology and increasing dependence upon the Internet offer the future malicious insider converged capabilities to conduct targeted physical sabotage within the cyber systems context. These blended attacks at the points where physical and virtual worlds converge have potentially severe implications for operations and security across all 16 critical infrastructure sectors. Increased insider capabilities aside, the critical change in the Mission Impossible future is the exponential increase the number of potential vulnerabilities as economic and technological imperatives drive critical assets from traditionally stand-alone, siloed systems to IP-based networks. In this world, the adversary is able to reach out and touch more systems and assets both faster and more anonymously than ever.

The workshop participants offered a corollary to the converged threat in that the future insider will have a dual threat capability owing to advanced cyber capabilities and physical proximity. They suggested that "proximity attacks" will become more and more frequent as Web 3.0 devices become a critical part of everyone's lives. In this future, a person need not be an employee or even a trusted business partner to be an insider. Twenty years from now when everyone has network cameras and carries Web 3.0 personal electronic devices, those seeking to do harm simply can use them as surrogates or "technical slaves." Because of technology, one's physical presence in a room makes them susceptible to this, for example, using Bluetooth technology to remotely turn on microphones and cameras. The subject matter experts commented that this can happen now, so what will the landscape look like in 20 years?

Challenges. The workshop participants outlined the following challenges for public and private critical infrastructure stakeholders in the Mission Impossible alternative future.

- A shifting threat landscape in light of Web 3.0 and "cloud" computing, e.g., "deperimeterization" and the proliferation of proximity attacks as part of the digital insider TTPs;
- Operational and cyber-related interdependencies that render every critical infrastructure and supporting industry as vulnerable as its weakest partner;
- The Internet "arms bazaar" that gives adversaries increasingly easy access to a wider array of attack tools;
- An ongoing lack of industrial policies and standards to defend against current and future insider threats;

- Overcoming policy, legal, technical, and public opinion issues associated with obtaining and analyzing relevant threat data via social media, physical, cyber, behavioral means;
- Obtaining well-targeted funding for governance and playing catch-up against a rapidly evolving threat. Key in this regard are risk-based and prioritized funding decisions to ensure resources are directed at the most appropriate aspects of the insider threat to a specific infrastructure or supporting asset;
- Globalization of the workforce; and
- Balancing employee trust and privacy issues (fear of "Big Brother") while dealing effectively with the insider threat.

Opportunities. The workshop participants outlined the following opportunities for public and private critical infrastructure stakeholders in the Mission Impossible alternative future.

- Converging the physical and cybersecurity management programs to defeat the advanced insider TTPs. If there a single significant attack is successful, public and private stakeholders may be more motivated to marshal resources and to resolve long-standing legal and technical roadblocks; and
- Learning from failures and best practices to make governance related to insider risk management more effective. This includes implementing robust threat information sharing and reporting procedures and mechanisms among all concerned public and private stakeholders.

Signposts and Indicators. The workshop participants identified the following indicators that can signal public and private critical infrastructure stakeholders that the Mission Impossible future may be emerging.

- An increase in the number of successful insider attacks;
- Insiders that should have been easy to detect and catch but were not;
- An increase in attack attempts, distinct from successful insider attacks. The environment is conducive to attacks because the insider knows the vulnerabilities inherent in a haphazard governance culture. By their actions, malicious actors tell us what is of value and critical;
- Failure to migrate from service-level agreements to best practices for insider threat programs. We are encouraged to migrate to the "cloud" because it increases security, but it does not in the context of infiltration and insider threats. "Cloud" providers to critical infrastructure should, by association, be considered critical infrastructure in themselves. Accordingly, they should be held to higher standards than simple service-level agreements provide. Having these standards in place, according to the workshop participants, would represent a fundamental game shift against the malicious insider;
- Lack of oversight and policy regarding outsourcing, particularly in the technical support and source code production arenas. According to the workshop participants, almost every objective study available asserts that third-party relationships involved insiders over whom organizations have little control;
- Inconsistent insider threat funding and protection standards across all U.S. critical infrastructure sectors;

- A continuation of a poor overall record of logging across all sectors, which typically only improves after incidents have occurred. In this regard, indicators of insider activity (e.g., trying to send out large amounts of data or a computer communications with an IP address that does not exist in the DNS cache) will vary depending on the type of infrastructure, the threat, and the intended method of compromise, making them difficult to isolate and analyze based on static rules; and
- Ongoing confusion as to what organizations are *allowed* to do with respect to employee privacy.

Table G-1 provides a summary of the in-depth findings for the Advantage Good Guys and Mission Impossible alternative futures.

Table G-1. Summary Findings for the Advantage Good Guys and Mission Impossible Alternative Futures

	Advantage Good Guys	Mission Impossible
Challenges	▪ Maintain effective governance in the face of constantly evolving threats ▪ Balance operations and security ▪ Manage relevant data ▪ Retain funding ▪ Monitor "consumerization" of insider threat ▪ Globalization of workforce ▪ Employee Trust as a counterpoint to globalization of the workforce	▪ Web 3.0 and "cloud" computing, e.g., "deperimeterization" of the threat ▪ Interdependencies that render critical infrastructure and supporting industries as vulnerable as the weakest partner ▪ The Internet "arms bazaar" ▪ Lack of policies and standards ▪ Policy, legal, and technical issues associated with obtaining and analyzing relevant threat data ▪ Risk-based funding for governance ▪ Globalization of the workforce. ▪ Balancing employee trust and privacy issues
Opportunities	▪ Establish best practices accepted by overseas partners ▪ Potential for lower costs (legal, insurance) ▪ Employee insider threat awareness training must continue to evolve	▪ Converging the physical and cybersecurity management programs ▪ Learning from failures and best practices
Signposts and Indicators	▪ Performance-based policies that include information sharing, standards, metrics, and deliverables ▪ Reduced number and severity of insider attacks ▪ Increased awareness and reporting on insider activity indicators ▪ Employee privacy laws that specifically address the many facets of mitigating insider threats to physical and cyber assets (primary and supporting) ▪ Emergence of a "human firewall" for reporting on insider activity indicators ▪ Standardized personnel policies ▪ Formalized education and training on insider threats	▪ Increased number of breaches ▪ Insiders that should have been easy to catch but were not ▪ Increased attack attempts, distinct from breaches ▪ Failure to migrate from service-level agreements to best practices for insider threat programs vis-à-vis "cloud" providers ▪ Lack of oversight and policy regarding outsourcing, particularly in the technical support and source code production arenas ▪ Inconsistent insider threat funding and protection standards ▪ Continuation of a poor overall record of logging ▪ Confusion as to what organizations are *allowed* to do vis-à-vis employee privacy

Strategic Surprises

Workshop participants identified the following strategic surprises that could bring chaos to the insider threat landscape and U.S. critical infrastructure during the next 20 years: [120]

[120] A strategic surprise is an unanticipated incident or event that causes significant disruption or damage to a critical infrastructure sector and/or supply chain. See the U.S. National Intelligence Council, *Disruptive Civil Technologies: Six Technologies with Potential Impacts on U.S. Interests Out to 2025,* Conference Report CR 2008-07, April 2008, www.fas.org/irp/nic/disruptive.pdf, accessed August 20, 2012, accessed March 15, 2012.

- An insider terrorist cyberattack. For example, an insider at a large industrial, chemical processing plant designs a "logic bomb" to shut down all of the critical valves and/or severely alter the system by simply commenting out one line of code. The workshop participants offered that this would not necessarily be a particularly sophisticated attack for the skilled, well-placed insider.
- A widespread "cloud" computing attack.
- Insiders having a direct gateway to the device of their choice via compromise of application ("app") stores, an inevitable threat landscape we have chosen for ourselves.
- A dramatic drop in cybersecurity funding as a knee-jerk reaction to a devastating physical attack.
- Contamination of assets and products in the Food and Agriculture, Water, and Healthcare and Public Health Sectors.
- Release or mixing of chemicals via cyberattack.
- "Logic bombs" planted by systems administrators that impact Healthcare and Public Health Sector. For example an employee could plant a "logic bomb" downloaded from the Internet on computers, causing computers to overheat and shut down critical HVAC systems.
- An asymmetric weapon attack on National Monuments and Icons Sector asset to render a symbolic landmark or place unusable for the foreseeable future and create deep psychological impact.
- To significantly damage the U.S. economy with one attack, one insider in a key financial clearing house manipulates critical functions such as the integrity of servers controlling time stamps for high frequency trading. In addition, one successful attack on a large, converged network hosting system could be equivalent to thousands of smaller attacks.

Future Analytic Considerations

The workshop participants noted that the security and operating standards of operations outside of the United States are major issues for U.S. critical infrastructure. Knowing which critical infrastructures to which our economy is wedded should be at the forefront in terms of protecting national security. In an increasingly global operating environment, this includes determining how to overcome the impacts of legal and cultural issues such as the "no one in my country would ever do this" mentality, especially with U.S. dependence on foreign countries for key inputs to our defense systems and critical infrastructure directly related to national security. The subject matter experts also expressed concern about the increased criminal use of the Banking and Finance Sector by terrorist organizations and nation-states via mobile banking and payments systems and financial fraud.

The workshop participants agreed that much more data collection, research, and analysis remain to be done regarding the motivations and drivers for would-be malicious insiders. Better visibility on both public and private industry threat detection programs, technology, and case histories would be good places to start in assembling quality analytic data.

Appendix H: NRE Coordination Approach

Coordination, both internal and external to DHS, has remained a priority throughout the development of the NRE. During the research and planning phase, DHS established a layered outreach approach in order to develop an NRE coordinated with interagency organizations by January 2013. The coordination began in February 2012 by creating an internal writing team and obtaining input and feedback within DHS. A Terms of Reference (TOR) was drafted, and external Departments, Agencies, and other organizations that could provide subject matter expertise on the information requirements driven by the key questions in the TOR were identified.

Each phase of the NRE development and coordination process illustrates an additional layer of fidelity in the coordination approach (Figure H-1). The research and planning phase included conducting an initial literature review, developing the TOR, and hosting the NRE Kickoff meeting to inform appropriate U.S. Government agencies about the NRE and request feedback on the TOR. The research and planning phase also included planning for the Alternative Futures Workshop and the Tabletop Exercises, which involved identifying and contacting subject matter experts in both the U.S. Government and the private sector and drafting an initial set of scenarios addressing insider threat and the U.S. critical infrastructure sectors.

(U)Figure H-1. NRE Development and Coordination Process

The workshop and exercises phase included developing additional scenarios and hosting one Alternative Futures development workshop and three Tabletop Exercises. These one-day events during April and May 2012 consisted of a small group of government and private sector subject matter experts. The workshop and exercise findings were incorporated into the NRE.

The analysis and coordination phase included planning the drafting and analysis of the NRE, conducting a risk assessment for selected critical infrastructure sectors and insider threats, identifying potential insider threat mitigation opportunities, and drafting chapters and appendices of the NRE.

The final phase of the NRE development process concluded with Interagency Coordination meetings. These meetings were held to provide an overview of initial analysis, fill information gaps, and coordinate findings with interagency organizations, as well as afford all agencies and participants the chance to provide comments in regard to their particular area of expertise. The following list includes those Agencies and/or groups that participated in some part of the NRE development or review process.

- Academia
  - Brown University
  - Carnegie Mellon University, Systems Engineering Institute, Computer Emergency Readiness Team/Insider Threat Center
  - College of William and Mary
  - The George Washington University
  - Harvard University, Belfer Center
  - National Defense University
  - Naval Postgraduate School
  - United States Military Academy at West Point
  - University of Miami
- Congressional Research Service
- Department of Defense
  - U.S. Fleet Cyber Command
  - U.S. Army, Computer Crime Investigative Unit
- Department of Energy
  - National Nuclear Security Administration (NNSA)
- Department of Homeland Security Components:
  - Immigration and Customs Enforcement
  - National Infrastructure Advisory Council
  - Office of Intelligence and Analysis
  - Transportation Security Administration
  - U.S. Coast Guard
  - U.S. Customs and Border Protection

  - U.S. Secret Service
  - National Protection and Programs Division
    - Office of Infrastructure Protection
    - Federal Protective Service
    - Office of Biometric Information Management
    - Office of Cybersecurity and Communications
      - U.S. Computer Emergency Readiness Team (US-CERT)
      - Industrial Control Systems Computer Emergency Response Team (ICS-CERT)
- Department of Transportation
- Department of Treasury
- Federal Bureau of Investigation
- Intelligence Community
  - Central Intelligence Agency
  - Defense Intelligence Agency
  - National Security Agency
  - Office of the Director of National Intelligence
  - Office of the National Counterintelligence Executive
- U.S. Nuclear Regulatory Commission
- National Insider Threat Task Force (Executive Order 13587)[121]
- National Laboratories
  - National Infrastructure Simulation and Analysis Center (NISAC)
- Numerous Private Sector Organizations
- Sector-Specific Agencies

[121] Executive Order 13587 was signed by the President on October 7, 2011. Section 6 requires establishing an "…interagency Insider Threat Task Force that shall develop a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as distinct needs, missions, and systems of individual agencies."

Appendix I: Subject Matter Expert Contributors to Tabletop Exercises and Alternative Futures Workshop

Terrorism Tabletop Exercise, April 20, 2012

	Subject Matter Experts	Organization	Team
1	**Asendorf, Patrick**	Nuclear Energy Institute	**Red**
2	**August, Jim**	CORE, Inc.	**Red**
3	**Ferezan, Dan**	Department of Transportation	**Blue**
4	**Garfinkel, Simson**	Naval Postgraduate School	**Red**
5	**Gupta, Ajay**	Gsesecurity, Inc.	**Red**
6	**Heffelfinger, Chris**	Researcher and Author	**Red**
7	**Lindner, Martin**	Carnegie Mellon U., CERT Insider Threat Center	**Blue**
8	**McIlvain, John**	Department of Energy	**Blue**
9	**Meyer, John**	DHS Office of Infrastructure Protection	**Red**
10	**Ostrich, John**	Department of Energy	**Blue**
12	**Richeson, Jon**	DHS Office of Infrastructure Protection	**Red**
14	**Spitzer, Lance**	SANS Institute	**Blue**
15	**Stock, Harley**	Incident Management Group	**Blue**
16	**Theis, Michael**	Carnegie Mellon U., CERT Insider Threat Center	**Red**
17	**Tobey, William**	Harvard University, Belfer Center	**Blue**
19	**Weese, Matt**	DHS Federal Protective Service	**Red**
20	**Zank, Arleen**	Coronado Group	**Blue**

Espionage Tabletop Exercise, April 25, 2012

	Subject Matter Experts	Organization	Team
1	**Andrews, John**	DHS Office of Intelligence and Analysis	**Blue**
2	**Axelrod, Warren**	Consultant	**Blue**
3	**Boroshko, Dave**	Federal Bureau of Investigation	**Red**
4	**Cappelli, Dawn**	Carnegie Mellon U., CERT Insider Threat Center	**Red**
5	**Caputo, Deanna**	Mitre Corporation	**Blue**
6	**Coleman, Kevin**	Technolytics	**Blue**
7	**Corbett, Steve**	DHS Office of Intelligence and Analysis	**Blue**
8	**Drissel, Anne**	US-VISIT	**Blue**
9	**Ertel, Thomas**	U.S. Fleet Cyber Command	**Blue**
10	**Fiedelholtz, Glenn**	DHS Office of Cybersecurity and Communications	**Red**
11	**Healey, Jason**	Atlantic Council	**Blue**
12	**Hemsley, Kevin**	DHS Industrial Control Systems (ICS)/ Computer Emergency Response Team (CERT)	**Blue**
13	**Jones, Jade**	National Security Agency	**Blue**
14	**Kellermann, Tom**	Trend Micro, Vice President for Cybersecurity	**Red**
15	**Kuehl, Daniel**	National Defense University	**Red**
16	**Link, Dave**	DHS Office of Cybersecurity and Communications	**Blue**
17	**Mander, Mark**	U.S. Army, Computer Crime Investigative Unit	**Red**
18	**Miller, Lorenzo**	DHS Office of Cybersecurity and Communications	**Red**
19	**Murphy, David**	DHS Office of Intelligence and Analysis	**Red**
20	**Rosenburgh, Dwayne**	National Security Agency	**Red**
21	**Shaw, Tim**	MAR, Inc., Chief Security Architect/ICS	**Red**
22	**Stock, Harley**	Incident Management Group	**Blue**
23	**Theis, Michael**	Carnegie Mellon U. CERT Insider Threat Center	**Red**
24	**Toecker, Michael**	Digital Bond, Inc.	**Blue**
25	**Vatis, Michael**	Steptoe & Johnson LLP	**Red**
26	**Woods, Randy**	Dow Chemical	**Red**

Corruption Tabletop Exercise, May 1, 2012

	Subject Matter Experts	Organization	Team
1	**Abela, Chris**	DHS Immigration and Customs Enforcement	**Red**
2	**Andreas, Peter**	Brown University	**Blue**
3	**Bach, Robert**	Consultant, Naval Postgraduate School	**Red**
4	**Bagley, Bruce**	University of Miami	**Blue**
5	**Bjelopera, Jerry**	Congressional Research Service	**Blue**
6	**Cabrera, Eduardo**	U.S. Secret Service	**Red**
7	**Cilluffo, Frank**	George Washington University	**Red**
8	**Felbab-Brown, Vanda**	Brookings Institution	**Red**
9	**Grayson, George**	College of William and Mary	**Blue**
10	**Hughes, Elena**	U.S. Coast Guard	**Blue**
11	**Leeman, Chris**	Transportation Security Administration	**Blue**
12	**Longmire, Sylvia**	Longmire Consulting	**Red**
13	**McMahon, Steve**	U.S. Secret Service Detailed to DHS/IP	**Blue**
14	**Peretti, Brian**	Department of Treasury	**Blue**
15	**Purdy, Andy**	Computer Sciences Corporation, Chief Cybersecurity Strategist	**Blue**
16	**Rouzer, Bret**	U.S. Coast Guard	**Blue**
17	**Stock, Harley**	Incident Management Group	**Red**
18	**Thompson, Eleanor**	U.S. Coast Guard	**Red**
19	**Whitley, Terry**	Shell Oil Company	**Red**

Alternative Futures Workshop, April 3, 2012

	Subject Matter Experts	Organization
1	**Cappelli, Dawn**	Carnegie Mellon U. CERT Insider Threat Center
2	**Caputo, Deanna**	Mitre Corporation
3	**Kellermann, Tom**	Trend Micro, Vice President for Cybersecurity
4	**Sanderson, Tom**	Center for Strategic and International Studies

Appendix J: Bibliography

Abrams, Marshall (the MITRE Corporation) and Joe Weiss (Applied Control Solutions). "Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services." July 23, 2008, http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

Agrell, J., Lindroth, Robert, and Norman, Andreas. "Risk, Information, and Incentives in Telecom Supply Chains." *International Journal of Production Economics v*90/1, July 8, 2004. www.uc3m.es/portal/page/portal/dpto_economia_empresa/home/seminars/Previous_years/Seminars_2008-2009/agrell.pdf.

Allen, Eddie. "Canada, Michigan announces new Detroit-Windsor Bridge." *Reuters,* June 15, 2012, www.reuters.com/article/2012/06/15/us-usa-canada-bridge-idUSBRE85E18X20120615.

Alert Enterprises. *NERC-CIP's Most Wanted. The Top Three Most Violated NERC-CIP Standards*. March 2011.

ALTERA Web site. *FPGAs.* July 2, 2012, www.altera.com/products/fpga.html.

Ambassador Bridge Web site. *Bridge Facts.* June 27, 2012, www.ambassadorbridge.com/IntlCrossing/BridgeFacts.aspx.

Anderson, Neil. *Securing Wireless Networks.* www.cisco.com/web/services/news/ts_newsletter/tech/chalktalk/archives/200802.html.

Association of Certified Fraud Examiners. *2012 Global Fraud Study: Report to the Nations on Occupational Fraud and Abuse.* www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf.

Aviationpros.com. "Baggage Handlers Arrested For Smuggling Tons Of Cocaine." June 7, 2012, http://www.aviationpros.com/news/10726451/baggage-handlers-arrested-for-smuggling-tons-of-cocaine, accessed August 27, 2012.

BPW Foundation. *Snapshot of Generation Y.* www.bpwfoundation.org/documents/uploads/SnapshotGenY.pdf.

Bureau of Transportation Statistics-Research and Innovative Technology Administration (RITA). *Border Crossing/Entry Data: Query Detailed Statistics*, updated March 2012. www.bts.gov/programs/international/transborder/TBDR_BC/TBDR_BCQ.html.

Business Wire. "LexisNexis identifies Top Trends in Health Care fraud, Waste and Abuse," *Business Wire*, February 16, 2012,

www.businesswire.com/news/home/20120216006254/en/LexisNexis-Identifies-Top-Trends-Health-Care-Fraud.

Canada-U.S.-Ontario-Michigan Border Transportation Partnership. *Border Transportation Partnership Planning/Need and Feasibility Study Report*. www.partnershipborderstudy.com/pdf/a_PNFStudyReport_FINAL_updatedpgnumbers.pdf.

Canadian National Railway Web site. "CN Renames Sarnia-Port Huron railway tunnel in honour of Paul M. Tellier." November 20, 2004, www.cn.ca/en/media-news-20041130a.htm.

Cappelli, Dawn M., Andrew P. Moore, Randall F. Trzeciak, and Timothy J. Shimeall. *Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition – Version 3.1*, Carnegie Mellon University (CMU)–Software Engineering Institute (SEI) CERT, January 2009.

Cappelli, Dawn, Andrew Moore, Randall Trzeciak. *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).* Westford, Massachusetts: Addison-Wesley, 2012.

Caputo, Deanna D., Greg Stephens, Brad Stephenson, and Minna Kim. *Human Behavior, Insider Threat, and Awareness: An Empirical Study of Insider Threat Behavior*. The MITRE Corporation, July 31, 2009.

Caputo, Deanna, Greg Stephens, and Marcus Maloof. "Detecting Insider Theft of Trade Secrets," *IEEE Security & Privacy (Vol. 7, No. 6)*, November/December 2009.

Carnegie Mellon University, Software Engineering Institute. *Capability Maturity Model Integration (CMMI)*. www.sei.cmu.edu/cmmi/.

Cashell, Brian, William D. Jackson, Mark Jickling, and Baird Webel. *The Economic Impact of Cyber-Attacks*, CRS Report for Congress RL32331. Washington, D.C.: The Congressional Research Service, Library of Congress, April 1, 2004.

Centers for Medicare and Medicaid Services. *National Health Expenditures 2010 Highlights.* www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/index.html?redirect=/NationalHealthExpendData/.

CERT Insider Threat Team. *Data Exfiltration and Output Devices – An Overlooked Threat*, October 17, 2011, www.cert.org/blogs/insider_threat/2011/10/data_exfiltration_and_output_devices_-_an_overlooked_threat.html.

Cisco. *2011 Cisco Connected World Report.* www.cisco.com/en/US/solutions/ns341/ns525/ns537/ns705/ns1120/2011-CCWTR-Chapter-3-All-Finding.pdf.

City of Houston. *Houston Facts and Figures.* www.houstontx.gov/abouthouston/houstonfacts.html.

Clancy, Mark G. "Cyber Threats to Capital Markets and Corporate Accounts," Congressional Testimony to the House Committee on Financial Services Subcommittee on Capital Markets and Government Sponsored Enterprises, June 1, 2012. www.hsdl.org/?view&did=711622.

Committee on Armed Services United States Senate. *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain.* Washington, D.C.: U.S. Government Printing Office, May 21, 2012. www.armed-services.senate.gov/Publications/Counterfeit%20Electronic%20Parts.pdf.
.

Committee on National Security Systems (CNSS). *National Information Assurance (IA) Glossary*, CNSS Instruction No. 4009, April 26, 2010. www.cnss.gov/Assets/pdf/cnssi_4009.pdf.

Connolly, Ceci. "Woman's Links to Mexican Drug Cartel a Saga of Corruption on U.S. Side of Border." *The Washington Post*, September 12, 2010. www.washingtonpost.com/wp-dyn/content/article/2010/09/11/AR2010091105687.html.

Deloitte and the National Association of State Chief Information Officers (NASCIOs). *The 2010 Deloitte-NASCIO Cybersecurity Study*, Deloitte Development LLC. www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy2010.pdf.

Depository Trust & Clearing Corporation (*DTCC*). *Safe, Secure, Setting New Standards: An Updated Report to the Industry on Business Continuity Planning*, DTCC White Paper, October 2011.

_____. "DTCC Urges Restart of Federal Program to Prevent Cyber Espionage," *Wall Street Technology*, June 4, 2012, at www.wallstreetandtech.com/technology-risk-management/dtcc-urges-restart-of-federal-program-to/240001415.

Donahue, Donald F. "The Public-Private Partnership and Supply Chain Resilience," Financial Services - Information Sharing and Analysis Center (FS-ISAC) Spring Member Meeting: Keynote Address, May 5, 2009. www.dtcc.com/downloads/leadership/speeches/Donal_F_Donahue_FS-ISAC_Speech.pdf.

Dubrawsky, Ida. "The "De-perimeterization of Networks," *Microsoft TechNet* September 12, 2007. http://technet.microsoft.com/en-us/library/cc512604.aspx.

Edmonds, James T. "Remarks Before the U.S. House Homeland Security Oversight, Investigations & Management Subcommittee." August 24, 2011. http:homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Edmonds.pdf.

Federal Bureau of Investigation. *Financial Crimes Report to the Public, Fiscal Years 2010-2011.* Washington, D.C.: U.S. Department of Justice, 2011. www.hsdl.org/?view&did=701476.

_____. "Testimony of Kevin L. Perkins, Assistant Director Criminal Investigative Division, Federal Bureau of Investigation," Washington, D.C.: U.S. Department of Justice," March 11, 2010. www.hsdl.org/?view&did=14472.

Fernández, D. "Current Situation of the Pharmaceutical Industry in Puerto Rico." Presentation at the Puerto Rico Health & Insurance Conference 2011, February 2, 2011, www.camarapr.org/PRHealth2011/presentations/PRH&I-Daneris_Fernandez.pdf.

Field, Tom. "Inside the Verizon Breach Report. Latest Trends on How Entities are Breached," *Bank Info Security,* August 9, 2010. www.bankinfosecurity.com/inside-verizon-breach-report-a-2826/op-1

Financial Services Information Sharing and Analysis Center (FS-ISAC). *Operating Rules,* March 14, 2011. www.fsisac.com/files/FS-ISAC_OperatingRules_2012.pdf.

_____. F*S-ISAC Frequently Asked Questions,* www.fsisac.com/faq/.

_____. *About the FS-ISAC.* www.fsisac.com/about/index.php.

Gelles, Michael G., David L. Brant, and Brian Geffert, *Building a Secure Workforce.* Deloitte Consulting LLP, 2008. www.deloitte.com/view/en_US/us/Industries/US-federal-government/764ef33b4010e110VgnVCM100000ba42f00aRCRD.htm.

Gelles, Michael and John Cassidy. *Security Along the Border: The Insider Threat,* Deloitte Consulting, LLP, 2011. www.deloitte.com/view/en_US/us/Industries/US-federal-government/federal-focus/homeland-security/a889e5fa3349d210VgnVCM3000001c56f00aRCRD.htm.

IMS National Sales Perspectives™. "Top U.S. Pharmaceutical Products by Spending." 2011. www.imshealth.com/deployedfiles/ims/Global/Content/Corporate/Press%20Room/Top-line%20Market%20Data/2010%20Top-line%20Market%20Data/2010_Top_Products_by_Sales.pdf.

InfoWorld Media Group. *Special Report. Insider Threat, Deep Dive: Combating the Enemy Within,* July 2010.

Info Security Web site. "Infosecurity Europe 2012—The insider threat, is it real?" www.infosecurity-magazine.com/view/25434/infosecurity-europe-2012-the-insider-threat-is-it-real/.

Info Security Web site. "Majority of firms plan to institute employee monitoring for social media use." www.infosecurity-magazine.com/view/26098/majority-of-firms-plan-to-institute-employee-monitoring-for-social-media-use.

Inspector General, U.S. Department of Health and Human Services. "Testimony of Daniel R. Levinson, Inspector General, U.S. Department of Health and Human Services to The United States Senate Committee on Finance," March 2, 2011. https://oig.hhs.gov/testimony/docs/2011/levinson_testimony_03022011.pdf.

International Air Transport Association. *The Impact of September 11 2001 on Aviation,* Switzerland, September 2011. www.iata.org/pressroom/Documents/impact-9-11-aviation.pdf.

Kellermann, Tom and Valerie McNevin. *Capital Markets and E-fraud: Policy Note and Concept Paper for Future Study*. World Bank Policy Research Working Paper 3586, May 2005.

Kellermann, Tom. "The Evolution of Targeted Attacks in a Web 3.0 World." July 2, 2012, http://cloud.trendmicro.com/the-evolution-of-targeted-attacks-in-a-web-3-0-world/.

King, Kathleen M. and Kay L. Daly. *Medicare and Medicaid Fraud, Waste and Abuse: Effective Implementation of Recent Laws and Agency Actions Could Help Reduce Improper Payments,* GAO-11-409T 9. Washington, D.C.: U.S. Government Accountability Office, March 2011. www.gao.gov/products/GAO-11-409T, accessed August 13, 2012.

Kramer, Lisa A., Richards J. Heuer, Jr., and Kent S. Crawford. *Technological, Social, and Economic Trends That Are Increasing U.S. Vulnerability to Insider Espionage,* Defense Personnel Security Research Center (PERSEREC) Technical Report 05-10. Monterey, CA: Defense Personnel Security Research Center, May 2005.

Lloyds TSB. *Money Mules.* www.lloydstsb.com/security/money_mules.asp.

Los Angeles Times. "TSA drug smuggling case is 'significant' security breach, feds say." *Los Angeles Times,* April 26, 2012, http://latimesblogs.latimes.com/lanow/2012/04/tsa-drug-smuggling-case-is-significant-security-breakdown-feds-say.html.

Marsh Consulting. *The Changing Face of Risk Management.* January 28, 2010. www.rimas.org.sg/files/The%20Changing%20Face%20of%20Risk%20Management.pdf.

Maxwell, Kenneth and Andrew Joyce. "Japan tries humor with 'Nuclear Boy' Fukushima," *The Wall Street Journal,* March 18, 2011. http://blogs.wsj.com/japanrealtime/2011/03/18/japan-tries-humor-with-nuclear-boy-fukushima/.

Melia, Michael. "Puerto Rico's Pharmaceutical Industry 'Terminally Ill." *Associated Press,* November 11, 2007, www.manufacturing.net/news/2007/11/puerto-ricos-pharmaceutical-industry-terminally-ill.

Metatach Corporation *An Overview of the National Academy of Sciences Report on Severe Space Weather and the Vulnerability of the U.S. Electric Power Grid*, January 11, 2009. www.wunderground.com/hurricane/2009/metatech2009.pdf

Michigan Department of Transportation. *Border Crossings in Michigan*, Jun 24, 2004. www.michigan.gov/documents/MDOT_Commission_Border_Briefing062404_95438_7.pdf.

Michigan Infrastructure & Transportation Association Web site. www.mi-ita.com/About/StClairRiverRailroadTunnel.aspx.

Miller, Melissa. "Flood of 2011 Anniversary: Corps Maintains Birds Point Levee Breech Saved Billions in Damages." *Southeast Missourian,* April 25, 2012. www.semissourian.com/story/1841366.html.

Moore, Andrew P., Dawn M. Cappelli and Randall F. Trazeciak. *The 'Big Picture' of Insider IT Sabotage Across U.S. Critical Infrastructures*, Carnegie Mellon University–Software Engineering Institute, May 2008.

National Protection and Programs Directorate/Office of Infrastructure Protection. *Appendix B: 2011 National Risk Profile,* Washington, D.C.: U.S. Department of Homeland Security, November 2011.

National Infrastructure Advisory Council. *Intelligence Information Sharing: Final Report and Recommendations,* January 12, 2012. www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-0110212.pdf.

National Institute of Standards and Technology (NIST). *NIST IR 7298 Revision 1: Glossary of Key Information Security Terms,* February 2011.

_____. *The NIST Definition of Cloud Computing, SP 200-145.* September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

_____. *Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication (SP) SP800-53 Revision 4 Information Security.* Gaithersburg, MD: U.S. Department of Commerce, February 2012. http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf.

National Transportation Safety Board. *EgyptAir Flight 990, Boeing 767-366ER, SU-GAP, 60 Miles South of Nantucket, Massachusetts, October 31, 1999,* Aircraft Accident Brief, NTSB/AAB-02/01. March 13, 2002. www.ntsb.gov/doclib/reports/2002/AAB0201.pdf.

North American Electric Reliability Corporation (NERC). *Cyberattack Task Force: Final Report,* May 9, 2012.

_____. *NERC CIP-004-4a Cyber Security Personnel and Training*, May 24, 2012.

Noonan, Thomas and Edmund Archuleta. *The National Infrastructure Advisory Council's Final Report and Recommendations on The Insider Threat to Critical Infrastructure*, Washington, D.C.: National Infrastructure Advisory Council, 2008.

Office of Infrastructure Protection. *National Infrastructure Protection Plan*, Washington, D.C.: U.S. Department of Homeland Security, 2009.

Office of the Inspector General, U.S. Department of Health & Human Services. "A Perspective on Fraud, Waste and Abuse within the Medicare and Medicaid Programs." Testimony of Gerald T. Roy, Deputy Inspector General for Investigations, before the U.S. House of Representatives Committee on Oversight & Government Reform, Subcommittee on Health Care, District of Columbia, Census and National Archives, April 5, 2011. http://oig.hhs.gov/testimony/docs/2011/Roy_Testimony_04052011.pdf.

Office of the National Counterintelligence Executive (ONCIX). *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collections and Industrial Espionage, 2009-2011.* Washington, D.C., October 2011.

PA Consulting Group Web site. *Managing the Threat of Espionage*, April 28, 2011. www.paconsulting.com/our-thinking/managing-the-threat-of-espionage/.

Pardis, John. "Strategic Command Missions Rely on Space." September 29, 2003, www.defense.gov/news/newsarticle.aspx?id=28408.

Patch, David. "Tunnels provide key U.S. Canada link from Detroit," *The Toledo Blade,* June 25, 2012, www.toledoblade.com/local/2012/06/25/Tunnels-provide-key-U-S-Canada-link-from-Detroit.html.

Ponemon Institute. *First Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies.* Traverse City, MI: Ponemon Institute LLC, July 2010. www.nacha.org/userfiles/File/Internet_Council/Resources/Ponemon%20cost%20of%20cybercrime.pdf.

Port Authority of Houston. *General Information: The Port of Houston.* www.portofhouston.com/geninfo/overview1.html#theport.

Qinghan, Xiao, Thomas Gibbons and Harvé Lebrun. "RFID Technology, Security Vulnerabilities, and Countermeasures," In *Supply Chain: the Way to Flat Organization,* Julio Ponce and Adem Karhoca (Eds.), January 2009. http://cdn.intechopen.com/pdfs/6177/InTech-Rfid_technology_security_vulnerabilities_and_countermeasures.pdf.

Reed, Michael. "Growth at Port of Houston Bodes Well for Job-Seekers" *Houston Regional News Bureau,* January 13, 2012. www.yourhoustonnews.com/news/favorable-trade-winds-ahead-growth-at-port-of-houston-bodes/article_b7863165-4409-51e2-a433-17e6e6b401f6.html.

Reuters. "Canada, Michigan announce new Detroit-Windsor bridge," June 15, 2012. www.reuters.com/article/2012/06/15/us-usa-canada-bridge-idUSBRE85E18X20120615.

Roberts, John. "GPS at Risk from Terrorists, Rogue Nations, and $50 Jammers, Expert Warns," *Fox News*, February 23, 2012, www.foxnews.com/scitech/2012/02/23/gps-emerging-threat/print.

SAS Institute, Inc. *Combating Health Care Fraud: State-of-the-art methods for detection and prevention of fraud, waste and abuse in the health care industry.* 2010. www.ucl.ac.uk/secret/events/event-tabbed-box/seminars-accordian/healthcare-fraud.

Shaw, Eric, Ph.D, Kevin G. Ruby, and Jerrold M. Post, M.D. "The Insider Threat to Information Systems: The Psychology of the Dangerous Insider," *Security Awareness Bulletin* No. 2-98, 1998. www.pol-psych.com/sab.pdf.

Silowash, George, Dawn Cappelli, Andrew Moore, Randall Trzeciak, Timothy J. Shimeall and Lori Flynn. *Common Sense Guide to Mitigating Insider Threats – 4th Edition*. Carnegie Mellon University (CMU)−Software Engineering Institute (SEI) CERT, December 2012.

Symantec Corporation. *2011 State of Security: Global Findings*, August 2011. www.symantec.com/content/en/us/about/media/pdfs/symc_state_of_security_2011.pdf.

The White House. *2010 National Security Strategy.* May 2010. www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

_____. *Executive Order 13587 – Structural Reforms to Improve the Security of Classified Networks and the responsible Sharing and Safeguarding of Classified Information*, October 7, 2011. www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net.

Trend Micro. *12 Security Predictions for 2012.* www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/sp_12-security-predictions-for-2012.pdf.

_____. *Server Defense for Virtual Machines*. August 2009.

_____. *Changing the Game for Anti-Virus in the Virtual Datacenter*. September 2012.

U.S. Department of Justice. *Testimony of Kevin L. Perkins, Assistant Director Criminal Investigative Division, Federal Bureau of Investigation,* March 11, 2010. www.hsdl.org/?view&did=14472.

U.S. Department of Homeland Security. *Strategy to Enhance International Supply Chain Security.* July 2007. www.dhs.gov/xlibrary/assets/plcy-internationalsupplychainsecuritystrategy.pdf.

_____. *Statement of Alan Bersin, Commissioner, Customs and Border Protection on 'Border Corruption: Assessing Customs and Border Protection and The Department of Homeland*

Security Inspector General's Office Collaboration in the Fight to Prevent Corruption, June 9, 2011. www.dhs.gov/ynews/testimony/testimony_1307549850535.shtm.

_____. *DHS National Preparedness Goal, First Edition*, September 2011. www.fema.gov/pdf/prepared/npg.pdf.

_____. *Insider Threat Mitigation Effective Practices*, December 2011.

_____. *Power Hungry: Prototyping Replacement EHV Transformers*, March 2, 2012. Accessed August 24, 2012, www.dhs.gov/power-hungry-prototyping-replacement-ehv-transformers.

_____. *Critical Infrastructure Cybersecurity and the Insider Threat*, July 30, 2012.

U.S. Government Accountability Office. *Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to be Consistently Addressed*, GAO-10-628. Washington, D.C.: U.S. Government Accountability Office, July 2010.

_____. *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks*, GAO-12-361. Washington, D.C.: U.S. Government Accountability Office, March 2012.

_____. *Cybersecurity: Threats Impacting the Nation*, GAO-12-666T. Washington, D.C.: U.S. Government Accountability Office, April 24, 2012. www.gao.gov/assets/600/590367.pdf.

U.S. National Intelligence Council. *The Threat to U.S. National Security Posed by Transnational Organized Crime*, No date. www.dni.gov/files/documents/Special%20Report_The%20Threat%20to%20U.S.%20National%20Security%20Posed%20by%20Transnational%20Organized%20Crime.pdf.

_____. *Disruptive Civil Technologies: Six Technologies with Potential Impacts on U.S. Interests Out to 2025*, Conference Report CR 2008-07, April 2008. www.fas.org/irp/nic/disruptive.pdf.

U.S. Office of Special Council. *About the Hatch Act Federal Employees.* www.osc.gov/hatchact.htm.

_____. *Filing a Hatch Act Complaint*. www.osc.gov/haFilingComplaint.htm.

_____. *Penalties*. www.osc.gov/haFederalPenalties.htm.

U.S. Security and Exchange Commission. *Pump and Dump Schemes*, March 12, 2001. www.sec.gov/answers/pumpdump.htm.

VERDASYS. *Protecting Against WikiLeaks Type Events and the Insider Threat.* January 2011. www.iseprograms.com/lib/Verdasys_WikiLeaks.PDF.

Verizon RISK Team. *2012 Data Breach Investigations Report.* 2012. www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.

Weiland, Robert M., Andrew P. Moore, Dawn M. Cappelli, Randall F. Trzeciak and Derrick Spooner. *Spotlight On: Insider Threat from Trusted Business Partners,* Carnegie Mellon University (CMU)–Software Engineering Institute (SEI) CERT, February 2012.

Current Risk Scenario References

AirSafe Web site. www.airsafe.com/events/airlines/american.htm.

American Association of Railroads. *The Economic Impact of America's Freight Railroads*, June 2012. www.aar.org/~/media/aar/Background-Papers/The-Economic-Impact-of-Freight.ashx.

Aviationpros Web site. "Baggage Handlers Arrested For Smuggling Tons Of Cocaine," June 7, 2012, www.aviationpros.com/news/10726451/baggage-handlers-arrested-for-smuggling-tons-of-cocaine.

BBC Web site. "Terror plot BA man Rajib Karim gets 30 years," March 18, 2011, www.bbc.co.uk/news/uk-12788224.

Bergman, C. and B.G. Petterson. "Radiation Applications and Waste Management: Taking the Final Steps." *IAEA Bulletin* 1/1994, www.iaea.org/Publications/Magazines/Bulletin/Bull361/36104683640.pdf.

City of Houston. *Houston Facts and Figures.* www.houstontx.gov/abouthouston/houstonfacts.html.

Edmonds, James T. "Remarks Before the U.S. House Homeland Security Oversight, Investigations & Management Subcommittee." August 24, 2011. http:homeland.house.gov/sites/homeland.house.gov/files/Testimony%20Edmonds.pdf.

Info Security Web site. "Russian hackers behind first successful US SCADA system attack," *InfoSecurity Magazine*, November 11, 2011. www.infosecurity-magazine.com/view/22153/russian-hackers-behind-first-successful-us-scada-system-attack-/.

International Air Transport Association. *The Impact of September 2011 on Aviation*. Switzerland. www.iata.org/pressroom/documents/impact-9-11-aviation.pdf.

Lloyds' Register Web site. www.lloydsregisterasia.com/sectors-we-serve/pdfs/iso-28000.pdf.

Los Angeles Times. "TSA drug smuggling case is 'significant' security breach, feds say," April 26, 2012, http://latimesblogs.latimes.com/lanow/2012/04/tsa-drug-smuggling-case-is-significant-security-breakdown-feds-say.html.

Mutzabaugh, Ben. "JetBlue flight diverts, pilot 'seemed like he went crazy," *USA Today*, March 27, 2012. http://travel.usatoday.com/flights/post/2012/03/jetblue-flight-diverts-to-amarillo-after-pilot-acts-crazy/657653/1.

National Agricultural Statistics Service. National Statistics for Milk. Washington, D.C.: U.S. Department of Agriculture. www.nass.usda.gov/Statistics_by_Subject/index.php.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*. www.911commission.gov/report/911Report.pdf.

Los Angeles Economic Development Corporation (LAEDC) and the Orange North-American Trade Rail Access Corridor (OnTrac) Joint Powers Authority. *OnTrac Trade Impact Study: National Economic Significance of Rail Capacity and Homeland Security on the Alameda Corridor East*, September 2003. www.cs.ucr.edu/~mart/177/ontrac_economic_impact_homeland_security_exec_sum.pdf.

Port Authority of Houston. *General Information: The Port of Houston.* www.portofhouston.com/geninfo/overview1.html#theport.

Reed, Michael. "Growth at Port of Houston Bodes Well for Job-Seekers" *Houston Regional News Bureau*, January 13, 2012. www.yourhoustonnews.com/news/favorable-trade-winds-ahead-growth-at-port-of-houston-bodes/article_b7863165-4409-51e2-a433-17e6e6b401f6.html.

Sobel, J., A.S. Khan, and D.L. Swerdlow. "Threat of a biological terrorist attack on the US food supply: the CDC Perspective," *Lancet* (2002).

Stanford Graduate School of Business. *Caution About Bioterror Attack on the U.S. Milk Supply*, June 2005. www.gsb.stanford.edu/news/research/pubpolicy_wein_bioterror.shtml.

Stephenson, John B. Testimony before the Subcommittee on Environment and Hazardous Materials, Committee on Energy and Commerce, House of Representatives. *Drinking Water: Experts Views on How Federal Funding Can Best Be Spent to Improve Security*, GAO-04-1098T. Washington, D.C.: U.S. Government Accountability Office, September 30, 2004: 8, http://gao.gov/assets/120/111280.pdf.

U.S. Department of Homeland Security. *National Infrastructure Protection Plan: Dams Sector*, 2011. www.dhs.gov/xlibrary/assets/nppd/nppd-ip-dams-sector-snapshot-2011.pdf.

U.S. Department of Homeland Security. *Dams Sector Security Awareness Guide: A Guide for Owners and Operators*, 2007. www.dhs.gov/xlibrary/assets/ip_dams_sector_securit_awareness_guide.pdf.

U.S. Department of Homeland Security Web site. *Dams Sector: Critical Infrastructure Sector Overview*. www.dhs.gov/dams-sector.

Weingart, Oliver G., Taja Schreiber, Conny Mascher, Diana Pauly, Martin B. Dorner, Thomas F.H. Berger, Charlotte Egger, Frank Gessler, Martin J. Lossner, Marc-Andre Avondet, and Brigitte G. Dorner. "The Case of Botulinum Toxin in Milk: Experimental Data: Abstract," *Applied and Environmental Microbiology* (April 2010). http:aem.asm.org/cpntent/76/10/3293.

Appendix K. Selected Insider Threat Authorities

Committees, Task Forces and Executive Authorities on Insider Threat

In 2011, the President signed Executive Order 13587 Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information. This order established multiple committees and task forces with responsibility for safeguarding the Nation's information from insider threats. These committee and task force responsibilities are outlined below and detailed in the attached Executive Order.

- **The Senior Information Sharing & Safeguarding Steering Committee** was established by Executive Order 13587 and is co-chaired by the Office of Management and Budget (OMB) and the National Security Staff (NSS). The Committee membership includes the Department of State, Department of Defense, Department of Justice, Department of Energy, Department of Homeland Security, Office of the Director of National Intelligence and the Information Security Oversight Office.
  - The Steering Committee is to establish goals, provide guidance and oversight, monitor compliance and report progress to the President. They are to develop program and budget recommendations, coordinate interagency development and implementation of priorities, policies and standards.
- **The Executive Agent for Safeguarding Classified Information on Computer Networks (EA)** is comprised of senior representatives of the Department of Defense and the National Security Agency.
  - The Executive Agent will develop effective technical safeguarding policies and standards with the Committee on National Security Systems (CNSS) that address the safeguarding of classified information within national security systems as well as the systems themselves.
  - The Executive Agent will conduct independent assessments and report results to the Steering Committee as well as reporting annually to the Steering Committee on the work of CNSS.
- **The National Insider Threat Task Force (NITTF)** is co-chaired by the Department of Justice and the Office of the Director of National Intelligence. The Task Force includes members from the Department of State, Department of Defense, Department of Justice, Department of Energy, Department of Homeland Security, Office of the Director of National Intelligence and the Information Security Oversight Office.
  - The Task Force is to develop a government-wide program for deterring, detecting, and mitigating insider threats and develop minimum standards and guidance for implementation of the program's policy.
  - In addition, the Task Force will conduct independent assessments of agency programs and implementation of policy and standards. The Task Force can provide assistance to agencies, as requested, including through the dissemination of best practices.
  - The Task Force will provide analysis of new and continuing insider threat challenges facing the United States Government.

- **The Classified Information Sharing and Safeguarding Office** was created within the office of the Program Manager for the Information Sharing Environment and will provide sustained, full-time focus on sharing and safeguarding classified national security information.
  - The Office will advise the EA for Safeguarding Classified Information on Computer Networks and NITTF on development of an effective program to monitor compliance with established policies and standards needed to achieve classified information sharing and safeguarding goals.
  - The Office will support the Senior Steering Committee.

Executive Order 13587 – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

By the authority vested in me as President by the Constitution and the laws of the United States of America and in order to ensure the responsible sharing and safeguarding of classified national security information (classified information) on computer networks, it is hereby ordered as follows:

Sec. 1. Policy. Our Nation's security requires classified information to be shared immediately with authorized users around the world but also requires sophisticated and vigilant means to ensure it is shared securely. Computer networks have individual and common vulnerabilities that require coordinated decisions on risk management.

This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the Federal Government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), and all classified information on those networks.

Sec. 2. General Responsibilities of Agencies.

Sec. 2.1. The heads of agencies that operate or access classified computer networks shall have responsibility for appropriately sharing and safeguarding classified information on computer networks. As part of this responsibility, they shall:

(a) designate a senior official to be charged with overseeing classified information sharing and safeguarding efforts for the agency;

(b) implement an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force established in section 6 of this order;

(c) perform self-assessments of compliance with policies and standards issued pursuant to sections 3.3, 5.2, and 6.3 of this order, as well as other applicable policies and standards, the results of which shall be reported annually to the Senior Information Sharing and Safeguarding Steering Committee established in section 3 of this order;

(d) provide information and access, as warranted and consistent with law and section 7(d) of this order, to enable independent assessments by the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force of compliance with relevant established policies and standards; and

(e) detail or assign staff as appropriate and necessary to the Classified Information Sharing and Safeguarding Office and the Insider Threat Task Force on an ongoing basis.

Sec. 3. Senior Information Sharing and Safeguarding Steering Committee.

Sec. 3.1. There is established a Senior Information Sharing and Safeguarding Steering Committee (Steering Committee) to exercise overall responsibility and ensure senior-level accountability for the coordinated interagency development and implementation of policies and standards regarding the sharing and safeguarding of classified information on computer networks.

Sec. 3.2. The Steering Committee shall be co-chaired by senior representatives of the Office of Management and Budget and the National Security Staff. Members of the committee shall be officers of the United States as designated by the heads of the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Information Security Oversight Office within the National Archives and Records Administration (ISOO), as well as such additional agencies as the co-chairs of the Steering Committee may designate.

Sec. 3.3. The responsibilities of the Steering Committee shall include:

(a) establishing Government-wide classified information sharing and safeguarding goals and annually reviewing executive branch successes and shortcomings in achieving those goals;

(b) preparing within 90 days of the date of this order and at least annually thereafter, a report for the President assessing the executive branch's successes and shortcomings in sharing and safeguarding classified information on computer networks and discussing potential future vulnerabilities;

(c) developing program and budget recommendations to achieve Government-wide classified information sharing and safeguarding goals;

(d) coordinating the interagency development and implementation of priorities, policies, and standards for sharing and safeguarding classified information on computer networks;

(e) recommending overarching policies, when appropriate, for promulgation by the Office of Management and Budget or the ISOO;

(f) coordinating efforts by agencies, the Executive Agent, and the Task Force to assess compliance with established policies and standards and recommending corrective actions needed to ensure compliance;

(g) providing overall mission guidance for the Program Manager-Information Sharing Environment (PM-ISE) with respect to the functions to be performed by the Classified Information Sharing and Safeguarding Office established in section 4 of this order; and

(h) referring policy and compliance issues that cannot be resolved by the Steering Committee to the Deputies Committee of the National Security Council in accordance with Presidential Policy Directive/PPD-1 of February 13, 2009 (Organization of the National Security Council System).

Sec. 4. Classified Information Sharing and Safeguarding Office.

Sec. 4.1. There shall be established a Classified Information Sharing and Safeguarding Office (CISSO) within and subordinate to the office of the PM-ISE to provide expert, fulltime, sustained focus on responsible sharing and safeguarding of classified information on computer networks. Staff of the CISSO shall include detailees, as needed and appropriate, from agencies represented on the Steering Committee.

Sec. 4.2. The responsibilities of CISSO shall include:

(a) providing staff support for the Steering Committee;

(b) advising the Executive Agent for Safeguarding Classified Information on Computer Networks and the Insider Threat Task Force on the development of an effective program to monitor compliance with established policies and standards needed to achieve classified information sharing and safeguarding goals; and

(c) consulting with the Departments of State, Defense, and Homeland Security, the ISOO, the Office of the Director of National Intelligence, and others, as appropriate, to ensure consistency with policies and standards under Executive Order 13526 of December 29, 2009, Executive Order 12829 of January 6, 1993, as amended, Executive Order 13549 of August 18, 2010, and Executive Order 13556 of November 4, 2010.

Sec. 5. Executive Agent for Safeguarding Classified Information on Computer Networks.

Sec. 5.1. The Secretary of Defense and the Director, National Security Agency, shall jointly act as the Executive Agent for Safeguarding Classified Information on Computer Networks (the "Executive Agent"), exercising the existing authorities of the Executive Agent and National Manager for national security systems, respectively, under National Security Directive/NSD-42 of July 5, 1990, as supplemented by and subject to this order.

Sec. 5.2. The Executive Agent's responsibilities, in addition to those specified by NSD-42, shall include the following:

(a) developing effective technical safeguarding policies and standards in coordination with the Committee on National Security Systems (CNSS), as re-designated by Executive Orders 13286 of February 28, 2003, and 13231 of October 16, 2001, that address the safeguarding of classified information within national security systems, as well as the safeguarding of national security systems themselves;

(b) referring to the Steering Committee for resolution any unresolved issues delaying the Executive Agent's timely development and issuance of technical policies and standards;

(c) reporting at least annually to the Steering Committee on the work of CNSS, including recommendations for any changes needed to improve the timeliness and effectiveness of that work; and

(d) conducting independent assessments of agency compliance with established safeguarding policies and standards, and reporting the results of such assessments to the Steering Committee.

Sec. 6. Insider Threat Task Force.

Sec. 6.1. There is established an interagency Insider Threat Task Force that shall develop a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices within agencies.

Sec. 6.2. The Task Force shall be co-chaired by the Attorney General and the Director of National Intelligence, or their designees. Membership on the Task Force shall be composed of officers of the United States from, and designated by the heads of, the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the ISOO, as well as such additional agencies as the co-chairs of the Task Force may designate. It shall be staffed by personnel from the Federal Bureau of Investigation and the Office of the National Counterintelligence Executive (ONCIX), and other agencies, as determined by the co-chairs for their respective agencies and to the extent permitted by law. Such personnel must be officers or full-time or permanent part-time employees of the United States. To the extent permitted by law, ONCIX shall provide an appropriate work site and administrative support for the Task Force.

Sec. 6.3. The Task Force's responsibilities shall include the following:

(a) developing, in coordination with the Executive Agent, a Government-wide policy for the deterrence, detection, and mitigation of insider threats, which shall be submitted to the Steering Committee for appropriate review;

(b) in coordination with appropriate agencies, developing minimum standards and guidance for implementation of the insider threat program's Government-wide policy and, within 1 year of the date of this order, issuing those minimum standards and guidance, which shall be binding on the executive branch;

(c) if sufficient appropriations or authorizations are obtained, continuing in coordination with appropriate agencies after 1 year from the date of this order to add to or modify those minimum standards and guidance, as appropriate;

(d) if sufficient appropriations or authorizations are not obtained, recommending for promulgation by the Office of Management and Budget or the ISOO any additional or modified minimum standards and guidance developed more than 1 year after the date of this order;

(e) referring to the Steering Committee for resolution any unresolved issues delaying the timely development and issuance of minimum standards;

(f) conducting, in accordance with procedures to be developed by the Task Force, independent assessments of the adequacy of agency programs to implement established policies and minimum standards, and reporting the results of such assessments to the Steering Committee;

(g) providing assistance to agencies, as requested, including through the dissemination of best practices; and

(h) providing analysis of new and continuing insider threat challenges facing the United States Government.

Sec. 7. General Provisions.

(a) For the purposes of this order, the word "agencies" shall have the meaning set forth in section 6.1(b) of Executive Order 13526 of December 29, 2009.

(b) Nothing in this order shall be construed to change the requirements of Executive Orders 12333 of December 4, 1981, 12829 of January 6, 1993, 12968 of August 2, 1995, 13388 of October 25, 2005, 13467 of June 30, 2008, 13526 of December 29, 2009, 13549 of August 18, 2010, and their successor orders and directives.

(c) Nothing in this order shall be construed to supersede or change the authorities of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended; the Secretary of Defense under Executive Order 12829, as amended; the Secretary of Homeland Security under Executive Order 13549; the Secretary of State under title 22, United States Code, and the Omnibus Diplomatic Security and Antiterrorism Act of 1986; the Director of ISOO under Executive Orders 13526 and 12829, as amended; the PM-ISE under Executive Order 13388 or the Intelligence Reform and Terrorism Prevention Act of 2004, as amended; the Director, Central Intelligence Agency under NSD-42 and Executive Order 13286, as amended; the National Counterintelligence Executive, under the Counterintelligence Enhancement Act of 2002; or the Director of National Intelligence under the National Security Act of 1947, as amended, the Intelligence Reform and Terrorism Prevention Act of 2004, as amended, NSD-42, and Executive Orders 12333, as amended, 12968, as amended, 13286, as amended, 13467, and 13526.

(d) Nothing in this order shall authorize the Steering Committee, CISSO, CNSS, or the Task Force to examine the facilities or systems of other agencies, without advance consultation with the head of such agency, nor to collect information for any purpose not provided herein.

(e) The entities created and the activities directed by this order shall not seek to deter, detect, or mitigate disclosures of information by Government employees or contractors that are lawful under and protected by the Intelligence Community Whistleblower Protection Act of 1998, Whistleblower Protection Act of 1989, Inspector General Act of 1978, or similar statutes, regulations, or policies.

(f) With respect to the Intelligence Community, the Director of National Intelligence, after consultation with the heads of affected agencies, may issue such policy directives and guidance as the Director of National Intelligence deems necessary to implement this order.

(g) Nothing in this order shall be construed to impair or otherwise affect:

(1) the authority granted by law to an agency, or the head thereof; or

(2) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals

(h) This order shall be implemented consistent with applicable law and appropriate protections for privacy and civil liberties, and subject to the availability of appropriations.

(i) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

BARACK OBAMA

THE WHITE HOUSE,
October 7, 2011.

Appendix L. External Reviews of this National Risk Estimate

Job well done by HITRAC and the expert participants.

It is, or should be, common knowledge by now that the most pervasive threat to our critical information infrastructure is the insider threat. Whether through malicious intent, social engineering, or careless circumvention of enterprise security policy, the vulnerabilities inherent in the human interface with our critical data and systems have been as frequently ignored as they have been exploited. DHS HITRAC's National Risk Estimate for "Risks to U.S. Critical Infrastructure from Insider Threat" should leave government and enterprise executives no more excuses for neglecting this addressable problem.

By presenting "alternative futures" and concrete scenarios about how trusted, corrupted or disgruntled insiders can cause substantial damage to various critical infrastructure systems and services, the NRE illustrates "no brainer" vulnerabilities for C-suite and risk management executives, provides templates for assessing risk based on likelihood, consequence, and human psychological factors, and points the way toward mitigation tactics and strategies.

Since at least 85% of our nation's critical infrastructure is owned and operated by the private sector, DHS is best able to serve its mission by keeping the drumbeat loud and true and give our critical sectors the tools they need to move from policies of denial to strategic plans for security. When characterizing the insider threat, DHS most trenchantly observes the challenge: "When Trust, Autonomy, and Malicious Intent Converge."

—**Greg Garcia**, President, Garcia Cyber Partners; The Nation's first DHS Assistant Secretary for Cyber Security and Communications, 2006-2008

I want to congratulate the team on a comprehensive report and a job well done. I have had the opportunity to read through the report and overall I found it to be filled with a lot of interesting information about insider threat. It documents well the overall methodology and approach to how conclusions were reached. I thought the references that supported the report were reasonably comprehensive and that they reflected the overall body of thinking in the area of insider threat. I found the findings and recommendations around insider to be reasonable and to have relevance to program developers who are responding to the Executive Order and looking to stand up or enhance programs. I appreciated the observations that insider threat programs are at best inconsistent. I have looked at the different programs in my work from a maturity perspective and I believe that the recommendations will be helpful to many.

I like the futurist approach. I wanted to read more, especially as it related to the continued evolution of technology, the generational changes in the workforce and the way business will be conducted. I'd like to see more analysis of the evolution of behavior in the virtual space and how it relates to internal verses external constraint. Also, we need to be exploring how behavior in the

"technological and non-technological" space could be used not just for monitoring but for new and progressive vetting.

Other topics to explore in this context include enterprise risk management, the assessment of business processes as a source of indicators and more robust discussion of role based access and mitigation strategies.

> **—Dr. Michael Gelles**, Director, Deloitte Consulting, LLP Federal practice in Washington, D.C., consulting in the areas of human capital management and systems and operations; author of *Building a Secure Workforce* (2008) and *Security Along the Border: The Insider Threat* (2011)