EXECUTIVE SUMMARY

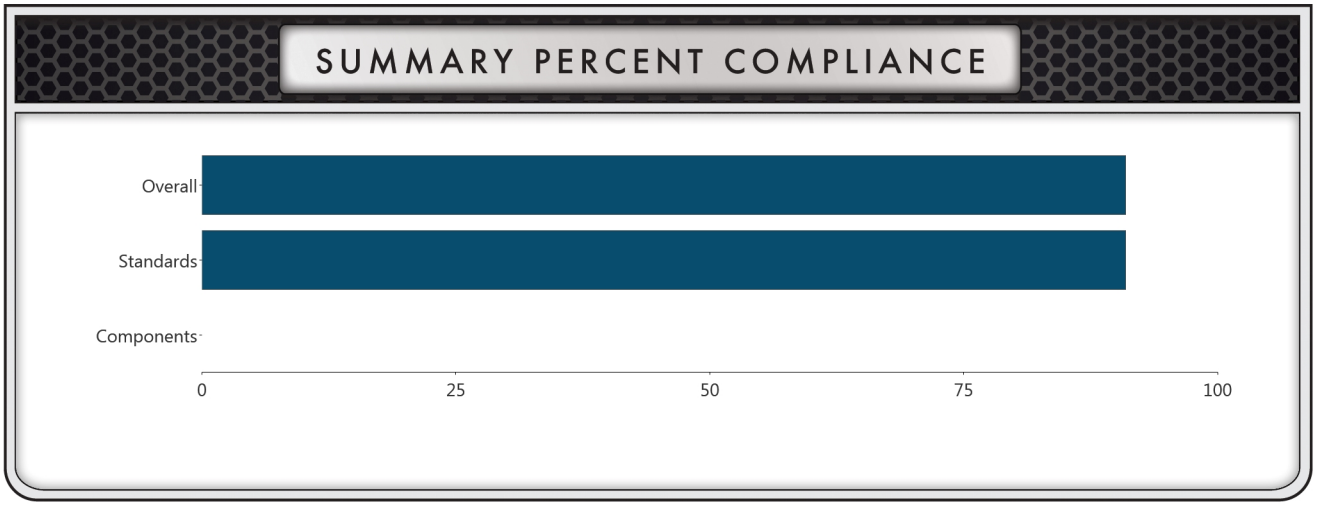
CONTROL SYSTEMS CYBER SECURITY EVALUATION

Homeland Security

High Level Cyber Security Assessment

2/1/2012

Assessor: J. Doe



DESCRIPTION OF ASSESSMENT

Cyber terrorism is a real and growing threat. Standards and guides have been developed, vetted, and widely accepted to assist with protection from cyber attacks. The Cyber Security Evaluation Tool (CSET) includes a selectable array of these standards for a tailored assessment of cyber vulnerabilities. Once the standards were selected and the resulting question sets answered, the CSET created a compliance summary, compiled variance statistics, ranked top areas of concern, and generated security recommendations.

The compliance summary charts below provide a high level overview of assessment results. The Summary Percent Compliance chart shows overall security status as well as a breakdown between compliance to selected standards (known as administrative) and compliance of those components depicted on the network diagram. The next two sets of graphs provide greater detail on compliance to selected standards and component compliance.

The Areas of Concern - Top Subject and Question section lists the five areas of greatest vulnerability. Addressing these areas quickly will provide the greatest return on investment.

EXECUTIVE SUMMARY

Enterprise Evaluation Executive Summary

This analysis identifies the cybersecurity posture of Industry City, CA. The review evaluated the business systems to identify what is performed well, what can be improved, and suggests options for consideration.

The approach used in reviewing Industry City, CA's cyber systems was the Enterprise Evaluation (EE), which includes a series of questions organized in ten categories derived from international, audit community, and federal government standards, and guidelines. The findings are presented based on the responses provided during the review. Notable Good Practices represent those practices of the organization that are areas of excellence. Most Critical Aspects for Improvement represent those issues that the organization should consider remedying immediately to mitigate vulnerabilities and minimize consequences of an egregious security breach. Moderately Critical Aspects for Improvement represent those issues that the organization should consider remedying in the near future in order to mitigate vulnerabilities and minimize consequences of a security breach. Finally, Least Critical Aspects for Improvement represent those issues that the organization should consider to improve security policies or incorporate generally accepted good practices.

This report does not make recommendations as to what should be changed. Instead, the report attempts to identify both notable good practices in place at Industry City, CA as well as gaps between current practices and what is possible with appropriate resources. Industry City, CA should conduct (or reevaluate) a risk assessment to determine if any gaps should be mitigated and to what extent. This assessment should be used to support risk-based decisions on policies, plans, procedures, and business systems operations.

EE is a vulnerability assessment rather than a risk assessment. Cyber vulnerabilities can often be mitigated through physical and human security measures. Given this reality, Industry City, CA should employ a robust risk management program that not only addresses threats, vulnerabilities, and consequences via cyber means, but also physical and human aspects. For example, while

issues such as the lockout of accounts are (and remain) vulnerabilities, their effects are reduced by the defense-in-depth approach of the physical and human security measures in place.

Cyber Threat: Malicious actors are increasingly acquiring information technology skills to potentially launch a cyber attack on the U.S. infrastructure. Cyber intruder groups already possess the necessary skills to launch a successful cyber attack and may be "talent-for-hire" available to terrorists, criminal organizations, and nation states. Attackers do not need to be technically savvy because free and commercial automated tools are simplifying attack methods.

Consequence of Attack On or Exploitation of Systems and Networks: If the business systems at this organization were compromised, the result could include the loss of sensitive data (e.g., intellectual capital, personal and health information) and the disruption of business operations. In addition, a compromise could provide a platform from which the process control network is attacked. Or, these networks could be exploited by malicious actors to attack other computers, facilities, and critical infrastructure through botnets.

Cybersecurity Posture (Vulnerability): A successful attack on the business systems is feasible through the Internet or other external connections (e.g., modems, wireless, portable devices, and media).

Company- or facility-specific information is often available on the Internet, and tools are readily available that automate search techniques for connections (e.g., Internet, wireless, and modems). Moreover, mature cyber attack tools (also available on the Internet) make common vulnerabilities easy to exploit by moderately skilled malicious actors unless perimeter security devices are properly configured and kept up to date (e.g., unless the option is turned off, firewalls will respond to reconnaissance attempts with information that enables cyber attack). An estimated ten new cyber vulnerabilities are discovered every day.

A common approach to cybersecurity is to secure the perimeter, leaving the internal network as a trusted environment. The actions of insiders (intentional or unintentional) then become an issue of concern. Unfortunately, unintentional consequences, introduced to systems through good intentions of trusted insiders, are known to have caused disruptions of operational business systems. In addition, system and network vulnerabilities are becoming more widely known and trends show that untargeted attacks, such as viruses, worms, and Trojans, are more prevalent. By opening e-mail attachments or visiting compromised web-sites, unsuspecting users can introduce malicious code to otherwise well-managed systems and networks.

Resources are available to assist in understanding and resolving consequential cyber attacks and incidents. Among them is the United States Computer Emergency Readiness Team (US-CERT), which, in partnership with the Multi-State Information Sharing and Analysis Center (MS-ISAC), published an information paper titled "Current Malware Threats and Mitigation Strategies," May 16, 2005. The following is an excerpt that summarizes the concern: "The nature of malicious code, or malware, (e.g., viruses, worms, bots) shifted recently… to actively seeking financial gain… [and] unfortunately, attackers have become very adept at circumventing traditional defenses such as anti-virus software and firewalls… Botnets are often the focal point for collecting the confidential information, launching Denial of Service attacks, and distributing SPAM. A bot, short for robot, is an automated software program that can execute certain commands. A botnet, short for robot network, is an aggregation of computers compromised by bots that are connected to a central 'controller.' … Botnets controlling tens of thousands of compromised hosts are common…" (Source: http://www.us-cert.gov/reading_room/malware-threats-mitigation.pdf; additional information can be found at the US-CERT home: http://www.uscert.gov/).

Cybersecurity practices that are performed well by Industry City, CA include: [Please insert the 3 or 4 sections that are of least concern here based on results from the Detailed Findings section of the report].

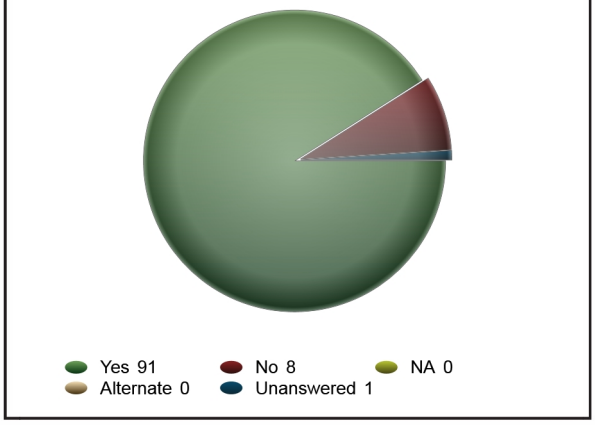
Several areas of concern make possible a successful cyber attack by malicious actors or a serious cyber incident. These include: [Please insert the 3 or 4 sections that are of greatest concern here based on results from the Detailed Findings section of the report].

Industry City, CA's most critical gaps are: [Please insert the Most Critical Aspects for Improvement here based on results from the Summary of Gaps and Options for Consideration section at the end of the report].

Company Comments
[Insert the most relevant high-level comments provided throughout the assessment here.]

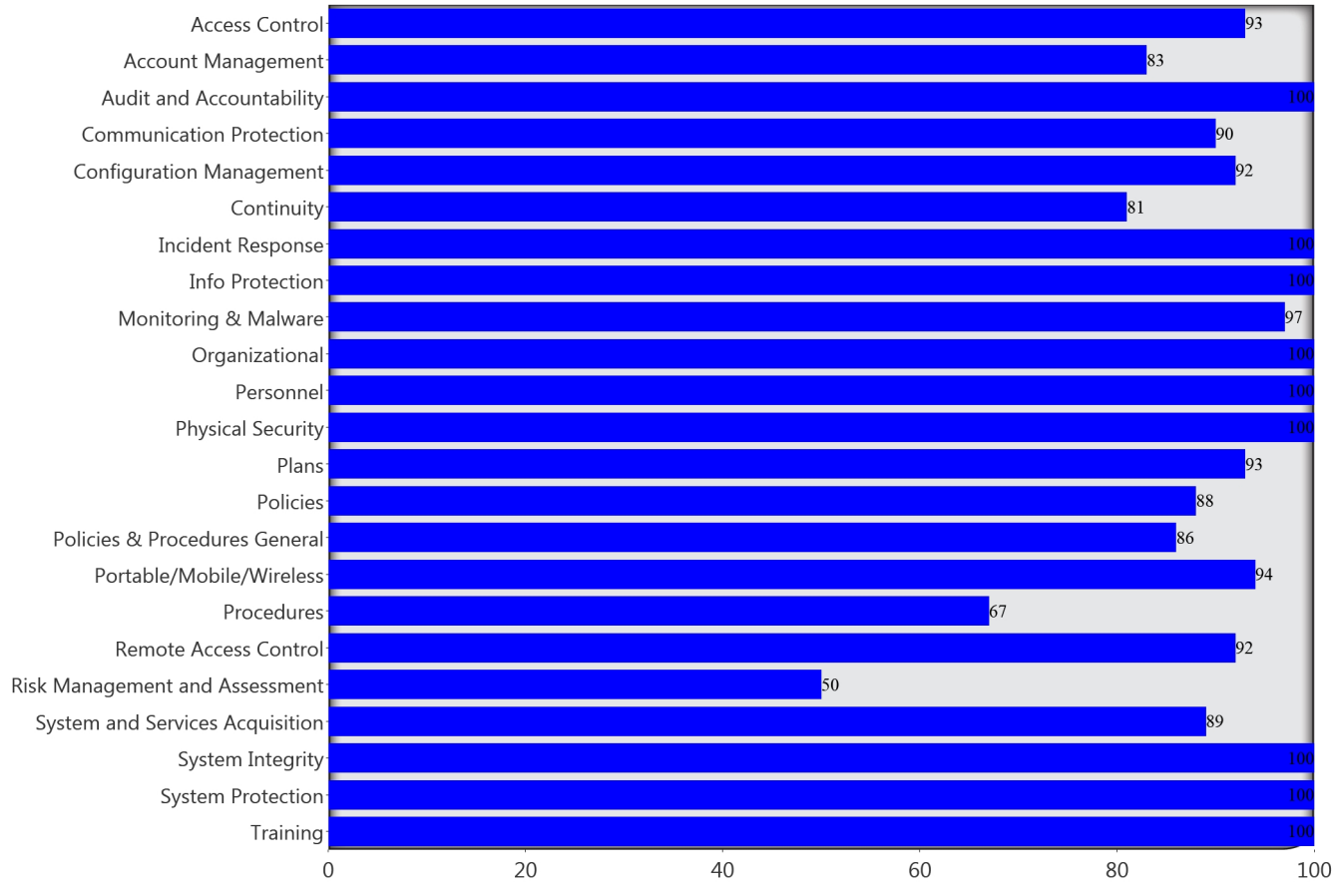
Evaluation Against Selected Standards and Question Sets

STANDARDS SUMMARY



STANDARD OR QUESTION SET

Key Questions



Areas of Concern
Top Subjects and Requirements

The top subject areas and requirements identify those areas where attention will either provide the most immediate impact or protect against the greatest vulnerabilities.

Top Subject Areas of Concern

1. Account Management
2. Procedures
3. Access Control
4. Remote Access Control
5. Communication Protection

Top Questions of Concern

1. Do the password policies stipulate rules of complexity, based on the criticality level of the systems to be accessed?
2. Is there an official assigned to authorize a user or device identifier?
3. Are identifiers selected that uniquely identify an individual or device?
4. Are the user identifiers assigned to the intended party or the device identifier to the intended device?
5. Are previous user or device identifiers archived?