INSIDER THREAT PROGRAM

MATURITY FRAMEWORK

National Insider Threat Task Force

Our collective efforts to address the insider threat require constant evaluation, fresh perspectives, and updated approaches to address current and future risk.

A MESSAGE FROM THE CO-DIRECTORS

Recent examples have shown the insider threat is a dynamic problem set – the threat landscape is continually evolving, technology is rapidly shifting, and organizations are changing in response to various pressures. Our collective efforts to address the insider threat require constant evaluation, fresh perspectives, and updated approaches to address current and future risk.

In furtherance of our joint efforts to mitigate insider threats, the National Insider Threat Task Force (NITTF), along with our executive branch partners, began looking at ways to strengthen the national effort. The result of this effort is this Insider Threat Program Maturity Framework (Framework). The Framework is designed to help all executive branch departments and agencies progress toward optimizing their insider threat program capabilities, recognizing that proactive insider threat programs are better postured to deter, detect, and mitigate insider threats before they reach a critical point and potentially harm national security.

The NITTF will continue to lead the national effort to counter the insider threat and support department and agency programs as they safeguard critical national security assets. This partnership is essential to our nation's ability to counter the threat from within.

R. Wayne Belk
NITTF Co-Director
Office of the Director of National Intelligence

Thomas D. Hix
NITTF Co-Director
Federal Bureau of Investigation

INTRODUCTION

The National Insider Threat Task Force (NITTF) is charged under Executive Order (EO) 13587 with reviewing and, when appropriate, adding to or modifying the Minimum Standards[1] and guidance in coordination with the executive branch departments and agencies (D/As) subject to the EO. The Minimum Standards provide the basic elements necessary to establish a fully functional insider threat program (InTP) and thereby serve as milestones in the InTP maturity process.

The insider threat is a dynamic problem set, requiring resilient and adaptable programs to address an evolving threat landscape, advances in technology, and organizational change. The effort requires continual evaluation and updated perspectives and approaches.

In furtherance of this effort, the NITTF has developed, in collaboration with executive branch D/As, an InTP Maturity Framework (hereafter referred to as "Framework") to enhance the Minimum Standards. The Framework identifies key elements within the Minimum Standards construct to enable D/As to increase the effectiveness of program functionality, garner greater benefit from InTP resources, procedures, and processes, and tightly integrate InTP procedures and objectives with their distinct missions and challenges.

The Framework consists of 19 elements aligned with the existing Minimum Standards topic areas. Each maturity element (ME) identifies a capability or attribute of an advanced InTP and provides amplifying information to assist programs in strengthening the effectiveness of the associated minimum standard. When using this Framework, InTPs should employ risk management principles tailored to meet the needs of their distinct workplace environment, technology infrastructure, and agency mission. InTPs also need to ensure compliance with their D/As' policies and regulations and all applicable legal, privacy and civil liberties rights, and whistleblower protections when evaluating and incorporating Framework elements into their programs.

The NITTF will continue to be a resource for InTPs as they work to advance their capabilities and resources in the effort to address the insider threat.

[1] The responsibilities for the NITTF and the basic requirements for insider threat programs are contained in EO 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, 7 October 2011; White House Memorandum on National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, 21 November 2012; and White House Memorandum on Compliance with the President's Insider Threat Policy, 19 July 2013.

INSIDER THREAT PROGRAM (InTP) MATURITY FRAMEWORK ELEMENTS

Senior Official / InTP Leadership

- **ME1:** o Exists as a dedicated effort, positioned in the D/A to ensure access to leadership to build support, identify resources, and integrate insider threat objectives within the D/A's mission and functions.
- **ME2:** Employs metrics to determine progress in achieving program objectives and to identify areas requiring improvement.
- **ME3:** Ensures InTP adapts to changes in law, policy, organizational structure, and information technology (IT) architecture.
- **ME4:** Employs risk management principles tailored to address the evolving threat environment and mission needs.

Program Personnel

- **ME5:** Includes stakeholders from a broad range of functional areas and others with specialized disciplinary expertise to strengthen InTP processes.
- **ME6:** Provides continuing education and training in appropriate fields and disciplines to help professionalize the insider threat cadre.

Employee Training & Awareness

- **ME7:** Provides training and materials to all employees addressing the full range of insider threats to create a culture of insider threat awareness and prevention within the D/A.

Access to Information

- **ME8:** Develops automated or scheduled processes for regular and timely receipt and integration of information from all relevant D/A stakeholders.
- **ME9:** Establishes procedures to receive notification with predictable frequency of information relevant to insider threat from other US Government (USG) and federal partner data holders.
- **ME10:** Employs documented processes to validate information sources and identify and assess the use of new information sources.

Monitoring User Activity

- **ME11:** Establishes a user activity monitoring (UAM) capability on all USG endpoints/devices and government-owned IT resources connected to USG computer networks accessible by cleared D/A personnel.
- **ME12:** Ensures UAM requirements are incorporated into D/A IT planning, design, and accreditation processes.
- **ME13:** Establishes capability to monitor the activity and conduct independent audits of InTP personnel with access to insider threat information and tools.

Information Integration, Analysis, & Response

- **ME14:** Employs data integration methodologies and advanced analytics to help detect anomalous activity and potential insider threats.
- **ME15:** Employs behavioral science methodologies to help identify indicators of potential insider threats.
- **ME16:** Employs risk scoring capability based on behavioral and workplace factors to assist with detection of anomalous activity and potential insider threats and in the application of tailored mitigation strategies.
- **ME17:** Documents procedures and agreements with other USG InTPs to request or refer information on insider threats of mutual concern.
- **ME18:** Employs case management tools to ensure integrity and effectiveness of the insider threat inquiry and response processes.
- **ME19:** Conducts routine exercises to improve integration, analysis, and response procedures and processes.

SENIOR OFFICIAL / INSIDER THREAT PROGRAM LEADERSHIP

ME1

Exists as a dedicated effort, positioned in the D/A to ensure access to leadership to build support, identify resources, and integrate insider threat objectives within the D/A's mission and functions.

- Establish countering insider threats as a core mission objective in protecting people, facilities, information, D/A mission, and national security.
- Promote development of insider threat-related competencies.
- Promote insider threat equities in all decision-making forums including policy, legal rights and protections, and resource allocation.

D/As that establish countering the insider threat as a core mission objective recognize the joint responsibility and commitment of D/A and InTP leadership to develop InTP infrastructure and personnel and promote the importance of addressing the insider threat at a level sufficient to create an effective and enduring Program. The InTP is organizationally placed to grant Program senior officials direct access to D/A leadership for support in the effort to detect, deter, and mitigate insider threat risk. D/A and Program leadership actively promote InTP equities in all decision-making forums to ensure Program interests and objectives are considered in D/A policies, regulations, and procedures. The joint responsibility and commitment extends to resourcing: a dedicated InTP budget line item provides for the staffing, analytic, and technology assets necessary to enable the Program to maintain and improve effectiveness in fulfilling its objectives.

ME2

Employs metrics to determine progress in achieving program objectives and to identify areas requiring improvement.

- Ensure insider threat metrics address specified InTP objectives and are a core component of the InTP's annual report to D/A leadership.
- Ensure metrics drive continual improvement in InTP procedures, processes, and capabilities and inform recommendations on policy, resources, and training.

Program senior officials can reinforce the value proposition and build support for the InTP by aligning InTP metrics with the D/A's mission and strategic plan. InTPs that use metrics to represent progress and challenges in protecting their D/As' information, resources, facilities, and personnel can better articulate and illustrate the central role of the Program in addressing these strategic objectives. An InTP Annual Report that incorporates metrics can alert D/A leadership to threats, gaps, and vulnerabilities and inform recommendations to improve policies, processes, procedures, capabilities, and training to mitigate the associated risks.

ME3

Ensure InTP adapts to changes in law, policy, organizational structure, and information technology (IT) architecture.

- Ensure InTP has visibility into D/A decision-making, legal and regulatory developments, and technology infrastructure advances.
- Regularly reviews agreements with Office of General Counsel (OGC), investigative elements, data-holders, and network service providers/ subscribers for consistency with applicable policy, law, and regulation.

It is crucial for InTPs in countering the insider threat to maintain compliance with changes in the policy, legal, regulatory, workforce, and technology environments of their D/A. The InTP can remain current through participation in D/A forums involved in policy-making, regulatory developments, and technology infrastructure advances to assess the impact of any changes on Program compliance and effectiveness. InTPs should periodically review and update their foundational documents, including insider threat policy, procedures, directives, and agreements. Program officials need to assess the potential impact of any changes on guidance to data holding offices and to existing Memoranda of Understanding/Memoranda of Agreement (MOUs/ MOAs) the InTP has established with network service providers/subscribers, investigative elements, and other agencies or components.

ME4

Employs risk management principles tailored to address the evolving threat environment and mission needs.

- Monitors continuing and new human and technical threats and vulnerabilities and modifies insider threat human behavioral assessment methodologies and technical indicators as needed.

The dynamic nature of human and technical insider threats and vulnerabilities require InTPs to maintain vigilance in managing risk. InTPs can work closely with experts in key functional area offices—for example, counterintelligence (CI), security, and information assurance (IA), among others—to maintain situational awareness on new and continuing challenges and make changes to insider threat procedures, processes, and capabilities to strengthen Program effectiveness in addressing potential threats and vulnerabilities. Programs also can employ risk management principals to enable flexibility in their application of human and technical resources against identified high priority and emerging threats.

PROGRAM PERSONNEL

ME5

Includes stakeholders from a broad range of functional areas and others with specialized disciplinary expertise to strengthen InTP processes.

- Staff InTP with a variety of disciplinary experience and perspectives to improve effectiveness in analysis and resolution processes.
- Promote direct participation and collaboration among diverse stakeholders to foster community and create program buy-in across the D/A.

InTPs can increase their effectiveness in countering the insider threat by developing a collaborative work environment with professionals from a variety of functional disciplines, either internally staffed or through agreement with external entities. The diversity of perspectives from personnel with experience in human resources (HR), CI, security, IA, legal, privacy and civil liberties, and law enforcement (LE) promotes enriched discussion and can help identify and contextualize anomalous behavior and the determination of response actions. The inclusiveness also can create a community of interest among stakeholders and reinforce a sense of shared responsibility in fulfilling the insider threat mission. Programs can also establish MOUs/MOAs with external elements for specialized support in areas not available within the D/A.

ME6

Provides continuing education and training in appropriate fields and disciplines to help professionalize the insider threat cadre.

- Identify career paths and training programs for the development of insider threat expertise and the advancement of InTP personnel.

The emphasis of the Minimum Standards on training and educational requirements underscores the importance of establishing competence in a broad range of knowledge and skills to effectively counter the insider threat. Continuing education and training for InTP personnel is vital for programs to maintain currency with methodologies in the disciplines underpinning the Program. Among the most important are behavioral sciences and analytic methodologies, data analytics, security, privacy and civil liberties, and CI. Programs can contribute to the overall goal of developing a professionalized national insider threat workforce by identifying professional development opportunities and career paths for InTP personnel with demonstrated knowledge, skills, and competencies in fields and disciplines central to countering the insider threat.[2]

EMPLOYEE TRAINING AND AWARENESS

ME7

Provides training and materials to all employees addressing the full range of insider threats to create a culture of insider threat awareness and prevention within the D/A.

- Strengthen the pro-active posture of the D/A through an on-going insider threat strategic communications campaign.
- Foster a sense of community and risk mitigation by positioning the program to include employee well-being and risk assurance.
- Promote open discussion about organizational vulnerabilities including workplace environment and technology use and risks.

InTP best practices affirm that an aware and properly trained workforce is the first line of defense in countering the insider threat. The workforce can act as a human sensor, alerting InTP personnel to anomalous activity long before it may be detected by other means. D/As can also strengthen their effectiveness in countering the insider threat by including the entire workforce, not only cleared employees, in insider threat awareness and prevention training. InTPs can drive cultural change within their D/As and build a culture of insider threat awareness and responsibility for reporting potential insider threats through communications campaigns. Programs can use these campaigns to build workforce knowledge and support, and dispel myths about what an InTP is and is not. To build support among the workforce, a noted best practice is to emphasize that early indicators of warning often are discovered through attentiveness to a colleague's personal well-being. Insider Threat awareness training media and messaging can incorporate anonymized, realistic stories to illustrate that reporting could lead to troubled individuals getting the assistance they need, as well as alert D/As to take action to address significant organizational vulnerabilities.[3]

---

[2] The NITTF recognizes the strategic importance of developing a professionalized insider threat workforce. Published in August 2017, the insider threat competency resource guide (CRG) is a keystone document applicable to all phases of the human capital lifecycle. The document was conceived as part of an effort to build an insider threat essential body of knowledge to define and codify key capabilities and competencies relevant to the insider threat workforce in the executive branch of the Federal Government and can positively influence how D/As recruit, select, train, develop, assess and retain the talent needed for the insider threat mission.

[3] Numerous insider threat training and awareness courses are available online from other D/As, including the Department of Defense, Defense Security Service, Center for Development of Security Excellence (CDSE) (www.cdse.edu). CDSE's offerings include insider threat and unauthorized disclosure toolkits, and online courses in CI, cyber, and a variety of security disciplines.

ACCESS TO INFORMATION

ME8

Develops automated or scheduled processes for regular and timely receipt and integration of information from all relevant D/A stakeholders.

ME9

Establishes procedures to receive notification with predictable frequency of information relevant to insider threat from other US Government and federal partner data holders.

ME10

Employs documented processes to validate information sources and identify and assess the use of new information sources.

- Establish repeatable and enduring electronic information access processes to strengthen the proactive posture of the InTP.
- Periodically review InTP information sources and past insider threat inquiries to assess the relevancy and utility of the sources and insider threat indicators.
- Work with stakeholders to identify new information sources and refine thresholds and triggers in light of changes in the threat, work, and technology environments.

InTPs can increase their effectiveness in countering the insider threat by developing a strong proactive posture in detecting issues of concern that may indicate potential threats. This involves regular and timely access to relevant data sources and the continual review and assessment of the types of data and evaluative criteria used in review and analysis of potential threats. A best practice among programs is periodic reassessment of the relevancy and utility of information sources and collaboration with stakeholders to identify new sources and types of information. Additionally, Program personnel should work closely with stakeholders and behavioral and analytic methodologists to assess insider threat indicators and refine thresholds and triggers in light of changes in the threat, work, and technology environments. In considering augmenting sources and types of information, programs need to consult with appropriate officials to ensure continuing compliance with applicable legal, privacy and civil liberties, and whistleblower protections.

MONITORING USER ACTIVITY

ME11

Establishes a user activity monitoring (UAM) capability on all USG end points/devices and government-owned IT resources connected to USG computer networks accessible by cleared D/A personnel.

- Assess for inclusion in monitoring all identified critical assets–classified and unclassified–which if degraded, stolen, or exploited would cause damage to the D/A or national security.
- Collaborate in the conduct of risk-based assessments of system and network vulnerabilities associated with the implementation of new technologies.
- Participate in reviews of the D/A's critical asset risk assessment process and consult with experts on risk assessment models.

ME12

Ensures UAM requirements are incorporated into D/A IT planning, design, and accreditation processes.

InTP senior officials can work with their technical, CI, and security counterparts to assess for inclusion in UAM all USG endpoints/devices, networks, and government-owned IT resources for identified critical assets–classified, controlled unclassified, and personally identifiable information–which if degraded, stolen, or exploited would cause damage to personnel, facilities and infrastructure, mission, or national security. Many programs have determined that by covering their unclassified systems, information is developed which may provide a deeper contextualization for identified anomalous behaviors in the workplace and on classified systems.

To maintain effectiveness, Program leadership can work with information security officials to ensure that insider threat UAM requirements are considered in the planning, design, upgrade, and accreditation of D/A computer systems and networks. InTP senior officials can participate in working groups that are responsible for the periodic review of the D/A's critical asset risk assessment process. They can also consult with experts on risk assessment models about the effectiveness of the technical and physical monitoring risk profile for insider threat.

ME13

Establishes capability to monitor the activity and conduct independent audits of InTP personnel with access to insider threat information and tools.

InTPs can also help reinforce the integrity and effectiveness of their mission by establishing a capability to ensure there is no misuse or mishandling of information accessed, developed, or retained by an InTP. The capability to conduct independent monitoring and auditing of InTP personnel – "watch the watcher" – can act as a check to ensure there is no misuse or mishandling of such sensitive information or, if this occurs, enable quick identification and mitigation actions.

INFORMATION INTEGRATION, ANALYSIS, & RESPONSE

ME14

Employs data integration methodologies and advanced analytics to help detect anomalous activity and potential insider threats.

- Incorporate capabilities to help manage and contextualize data and identify, isolate, and respond to potential threat indicators.

D/As, especially those with a large or geographically-dispersed workforce and diverse sources of insider threat-relevant information, can increase InTP effectiveness through the use of data aggregation and normalization utilities and advanced analytic tools. These utilities can help manage large data volume as a first step in establishing a baseline from which to identify anomalous behavior. Data analytic tools can help insider threat analysts to contextualize the behavior in supporting decisions to conduct inquiries, refer matters to response elements, and/or develop mitigation strategies. While there are many tools that can provide these capabilities, InTP officials should consider working with their counterparts in IA to survey the existing suite of tools employed by their D/A to determine if there is a preexisting capability that can serve InTP needs. Additionally, the IA team may also be able to provide guidance and assistance in assessing which data utilities and analytic tools might be appropriate to acquire if not currently available in house.

ME15

Employs behavioral science methodologies to help identify indicators of potential insider threat.

- Identify internal or external sources of behavioral sciences expertise to incorporate personal and environmental factors in threat identification, assessment and response.

The human-centric nature of the insider threat issue increases the importance of incorporating behavioral science perspective and expertise into InTP activities. Each employee responds to events and conditions in their work and personal lives differently—that response, positive or negative, is a key concern for an InTP. A program with access to personnel with behavioral sciences expertise, either through internal D/A or affiliated resources, can strengthen its capabilities to identify and assess types of concerning behavior, contextualize the behavior, discern unconscious biases and propose alternative hypotheses. Additionally, personnel with this expertise may provide additional context and insight into social/cultural mores that may impact resulting mitigation strategies and furnish advice during periodic revisions to insider threat indicators, triggers, and thresholds.

ME16

Employs risk scoring capability based on behavioral and workplace factors to assist with detection of anomalous activity and potential insider threats and in the application of tailored mitigation strategies.

- Uses a risk scoring capability to refine thresholds and triggers; analyze large data sets for threat pattern recognition; and in the application of InTP resources to identified risks.

InTPs in D/As with many employees, disparate data sources, and large volumes of data can use risk scoring technologies to help manage the multi-source information flow, primarily through establishing baselines to help detect anomalous activity or concerning behavior. Some risk scoring technologies have archive features that can support longitudinal analysis, important in detecting concerning patterns that appear over time. Some risk scoring technologies have archiving features that can support longitudinal analysis, important in detecting concerning patterns that appear over time.

ME17

Documents procedures and agreements with other USG InTPs to request or refer information on insider threats of mutual concern.

- Exchanges of information of insider threat concern with other D/As, in accordance with D/A authorities and applicable laws, regulations, and whistleblower, privacy and civil liberties protections. **Does not apply to 811 investigative referrals to the Federal Bureau of Investigation (FBI).**

The mobility of the federal government workforce requires the National Insider Threat Community be mindful that concerning behavior detected by one InTP may impact another D/A, thereby requiring a mechanism to share such information with counterparts. Though there is no national policy or directive, InTPs can establish MOUs/MOAs with specified D/As to refer or provide upon request concerning information, which may be relevant to a current or future inquiry. In establishing such agreements, Program senior officials need to consult with their general counsel and privacy and civil liberties offices to ensure compliance with agency authorities and applicable laws, regulations, privacy and civil liberties, and whistleblower protections. These agreements do not apply to investigative and 811 referrals to the FBI.

INFORMATION INTEGRATION, ANALYSIS, & RESPONSE

ME18

Employs case management tools to ensure the integrity and effectiveness of the insider threat inquiry and response processes.

- Facilitates maintaining an accurate and historical record of inquiry and response activity for longitudinal analysis.

Insider threat indicators of warning often prompt inquiries that are quickly resolved without the need for response. However, over time the accumulation of indicators, if documented, may suggest a pattern of activity that warrants further inquiry or action. Case management and workflow tools can increase the effectiveness of InTPs in providing the ability to manage the complete inquiry lifecycle and conduct longitudinal analysis to detect concerning patterns of behavior that appear over time.

ME19

Conducts routine exercises to improve integration, analysis, and response procedures and processes.

- Schedule periodic exercises that pose various scenarios to test insider threat inquiry and response action procedures, help assess and calibrate current criteria and thresholds, and identify gaps and deficiencies.

InTPs can use periodic exercises to improve their effectiveness in conducting inquiry and response processes outlined in their operations procedures. Such exercises can increase familiarity with all the related functional perspectives and build a best practices, multidisciplinary approach in analyzing behavioral anomalies. Programs can design these exercises to test the adequacy of insider threat indicators, triggers, and thresholds, as well as the measures and safeguards in place to ensure compliance with D/A policy and applicable laws and privacy and civil liberties rights. Programs can use the results of these exercises to inform changes to InTP processes and procedures, insider threat indicators, triggers, and thresholds, and recommendations to address identified vulnerabilities that put the D/A at risk.

The insider threat is a dynamic problem set, requiring resilient and adaptable programs to address an evolving threat landscape, advances in technology, and organizational change.