National INSIDER THREAT Task Force

ADVISORY: Insider Threat Competency Resource Guide

NITTF - ADV– 2017 – 01

DATE: August 30, 2017

PURPOSE:

The attached competency resource guide (CRG) is designed for use with the various components of the human capital lifecycle, and can positively influence how departments and agencies recruit, select, train, develop, assess, and retain talent needed to achieve the insider threat mission. In turn, this will advance efforts to professionalize the insider threat workforce.

BACKGROUND:

This CRG addresses key work activities and competencies required to deter, detect, and mitigate insider threats. It was developed as part of an effort to build an insider threat essential body of knowledge that defines and codifies key capabilities and competencies relevant to the insider threat workforce in the executive branch of the federal government.

The National Insider Threat Task Force (NITTF) led development of the CRG and partnered with the Office of the Assistant Director of National Intelligence for Human Capital through all phases of information collection, research and analysis, drafting, review, feedback, and validation. The CRG was developed after examining an assortment of insider threat-related position descriptions, and then deliberated in focus group workshops attended by insider threat personnel from 27 agencies in the executive branch. It was subsequently revised and then coordinated for additional vetting and review by departments and agencies in the IC, and validation by the broader insider threat community of interest in the federal government via job analysis surveys and questionnaires. A final editing and restructuring led to the attached version.

GUIDANCE:

This CRG applies to Intelligence Community (IC) employees who perform insider threat work, regardless of IC component, mission category, or occupational group. It may also be used for employees of non-IC federal agencies performing insider threat activities. The CRG identifies high-level work activities, core and technical competencies, and associated knowledge, skills, and abilities (KSAs) that can be applied across all phases of the insider threat human capital lifecycle: workforce planning, recruitment, selection, training/development, certification/ assessment, and performance management.

The insider threat CRG is linked to relevant competencies in Intelligence Community Directive (ICD) 610, *Competency Library for the Intelligence Community Workforce.* Though tied to ICD 610, this CRG was intentionally developed and written for broad applicability to, and use by, insider threat programs across the federal government. Its utility is not limited to the IC. It may be applied to insider threat personnel in the Department of Defense (DoD) and federal partner (non-Title 50) departments and agencies.

Generally speaking, CRGs are composed of three main components: (1) key work activities that describe work in a given occupation or specialty area, (2) the core, technical, and values-based competencies drawn from the larger IC competency library, required for successful completion of the work in that occupation or specialty area, and (3) the KSAs associated with each competency. In this CRG, these components distinguish the duties particular to insider threat program positions and describe the characteristics needed to perform these duties, regardless of the incumbent's functional or specialty area. The CRG also provides a common language through which the realm of insider threat work can be recognized, evaluated, and discussed across the IC and federal government. It helps establish responsibility and performance expectations among employees and their supervisors, and serves as a foundation for a variety of human capital management initiatives.

Insider threat programs draw upon the strengths and unique characteristics of the various disciplines represented within their programs, such as counterintelligence, security, information technology, human resources/human capital, behavioral science, etc. Program managers and their supporting human capital offices should use the insider threat competencies and KSAs in defining their human capital requirements, but they must also understand that the CRG may not be inclusive of all competencies relevant to certain insider threat occupations or positions.

This CRG is part of the larger IC competency library. Departments and agencies building position descriptions and vacancy announcements can leverage additional CRGs, competencies, or capabilities based on their agency-specific and position-specific human capital requirements. For example, a counterintelligence position might require a select set of competencies identified in this resource guide, as well as several technical competencies related to the technical area the position supports that are found elsewhere in the IC competency library.

As explained in the background section above, the CRG was developed in a collective, federated manner. It offers a broad array of key work activities, competencies, and KSAs that provide a good foundation for describing the work of insider threat personnel within the IC and across the federal government as a whole. Still, some departments and agencies may need to define additional or new KSAs for specific applications. To the extent that these applications will be used to make personnel decisions, consideration should be given to developing them in accordance with the *Uniform Guidelines on Employee Selection Procedures*[1], the *Principles for the Validation and Use of Personnel Selection Procedures*[2], and other relevant guidance.

Insider threat personnel and their supporting human capital offices should note that this CRG represents a snapshot in time. As mission needs evolve and new work roles or jobs are created to meet these needs, it may become necessary to update and refine the key work activities, competencies, and KSAs. Such changes will lead to gradual evolution of the CRG, with updates being vetted, validated, and approved via a governance process.

This document and the CRG have been through Office of the Director of National Intelligence classification review and pre-publication review. They were cleared for release as UNCLASSIFIED.

NITTF POC: Queries about this advisory should be directed to NITTF_TRAINING@dni.gov.

R. Wayne Belk

R. Wayne Belk
Director

Attachment:
Insider Threat Competency Resource Guide

[1] Uniform guidelines on employee selection procedures. (1978). *Federal Register, 43, 38290-38315*.
[2] Principles for the validation and use of personnel selection procedures. (4th ed., 2003). Bowling Green, OH: *Society of Industrial-Organizational Psychology.*

Competency Resource Guide for Insider Threat

A. AUTHORITY: The National Security Act of 1947, as amended; and other applicable provisions of law.

B. PURPOSE: This Competency Resource Guide (CRG) for Insider Threat provides the established labels and definitions of competencies developed for employees in various occupational groups and mission budget categories performing insider threat related work. The competencies in this guide are drawn from the overarching IC competency library but may not be inclusive of all competencies relevant to certain insider threat occupations. Additional CRGs, IC competencies, or capabilities may be leveraged to describe the requirements of a specific position or occupation. For example, a counterintelligence position might require a select set of competencies identified in this resource guide as well as several technical competencies related to the technical area the position supports that are found elsewhere in the IC competency library.

C. APPLICABILITY: This CRG is applicable to all IC employees who perform insider threat work, regardless of IC component, mission category, or occupational group. It may also be instructive to, though not directive for, employees of non-IC federal agencies performing insider threat activities.

D. BACKGROUND: This CRG was developed in accordance with the procedures outlined in Chapter 4 of the *Intelligence Community Competency Handbook*. Please refer to Handbook for more information on the structure and purpose of the IC Competency Library and its associated resource guides, and how to apply the IC competencies in programs across the human capital lifecycle. Future CRGs will be available through the Office of the Director of National Intelligence online Competency Library Resource tool.

E. **COMPETENCY RESOURCE GUIDE TABLES:** The following tables are included in this CRG:

1. Table 1: Provides a definition of Insider Threat and the key work activities that Insider Threat professionals perform on the job.
2. Table 2: Summarizes the CRG by providing a list of the technical expertise competencies and other capabilities relevant to Insider Threat.
3. Table 3: Provides the established core competencies for all IC employees.
4. Table 4: Provides the Insider Threat-specific knowledge, skills, and abilities (KSAs) linked to IC Core, Supervisory & Managerial, and Senior Officer competencies.

5. Table 5: Provides Insider Threat-specific KSAs linked to technical expertise competencies.
6. Table 6: Provides other relevant Insider Threat-specific competencies linked to KSAs.

Table 1. Definition and Key Work Activities for Insider Threat

Definition: This CRG addresses activities to deter, detect, and mitigate insider threats. EO 13587 states that an insider threat is the threat that an insider will use her/his 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. *Note: Some departments and agencies (D/A) have expanded their insider threat programs to include deterring, detecting, and mitigating workplace violence and suicide. While EO 13587, the National Policy, and Minimum Standards do not specify these two issues, the contents of this CRG -- key work activities, core and technical competencies, and KSAs -- are broad enough to cover them should a D/A choose to do so.*

Key Work Activities:

1. **Conduct operational activities in response to potential insider threats**: Insider threat professionals must understand insider threat risks, vulnerabilities, and indicators to:
    - **Gather**: Identify, receive, and ingest data on potential insider threat incidents from various sources following established policies and procedures.
    - **Analyze**: Examine, integrate, interpret, and evaluate gathered data on potential insider threats using analytic tools, techniques, and methods.
    - **Assess**: Interpret data and intelligence analyses, test hypotheses, prioritize alternatives, and contextually frame findings and conclusions.
    - **Respond**: Conduct inquiries or investigations, as situations dictate, following established policies and procedures.
    - **Report**: Document, classify, and properly handle insider threat information, and report and/or refer potential insider threat incidents to relevant stakeholders, departments, and/or agencies following established policies and procedures.

2. **Counsel stakeholders on insider threat incidents and programmatic issues**: Insider threat professionals must have the ability to:
    - Advise program stakeholders and senior officials to facilitate review, response, and resolution of insider threat incidents and programmatic issues.
    - Provide technical guidance and/or direct support to program stakeholders requiring assistance in matters related to insider threats.

3. **Establish, implement, and review policies and procedures**: Insider threat professionals must have the ability to:
    - Establish, implement, and/or evaluate departmental/agency policies and procedures for coordinating insider threat program efforts with other mission areas consistent with protections for privacy and civil liberties of the workforce.
    - Establish, implement, and/or evaluate insider threat program standard operating procedures (SOPs) consistent with laws, policies, and regulations related to collection, retention, and dissemination of insider threat information.

4. **Execute insider threat awareness training requirements:** Insider threat professionals must have the ability to:
   - Prepare and conduct briefings, or otherwise offer training to their department/agency workforce to promote awareness of potential insider threats and reporting requirements.
   - Prepare, conduct, and evaluate briefings and required training for insider threat program personnel to implement the department/agency insider threat program.

5. **Evaluate program effectiveness**: Insider threat professionals must have the ability to:
   - Facilitate the systematic assessment and evaluation of insider threat risks and vulnerabilities, insider threat trigger development, and efforts to effect early detection.
   - Promote continuous improvement to the department or agency's insider threat program by evaluating the program's plan, policies, procedures, and metrics.
   - Conduct reviews, surveys, and assessments to determine compliance with established policies and procedures, as well as the effectiveness of training in raising insider threat awareness.

6. **Manage resources**: Insider threat professionals must have the ability to:
   - Identify, justify, coordinate, and secure financial/budgetary resources required to execute the insider threat program.
   - Identify, coordinate, and/or manage personnel and physical resources (e.g. facilities, hardware, software) required to successfully pursue insider threat mission and/or roles and responsibilities.

Table 2. Competency Resource Guide Summary for Insider Threat

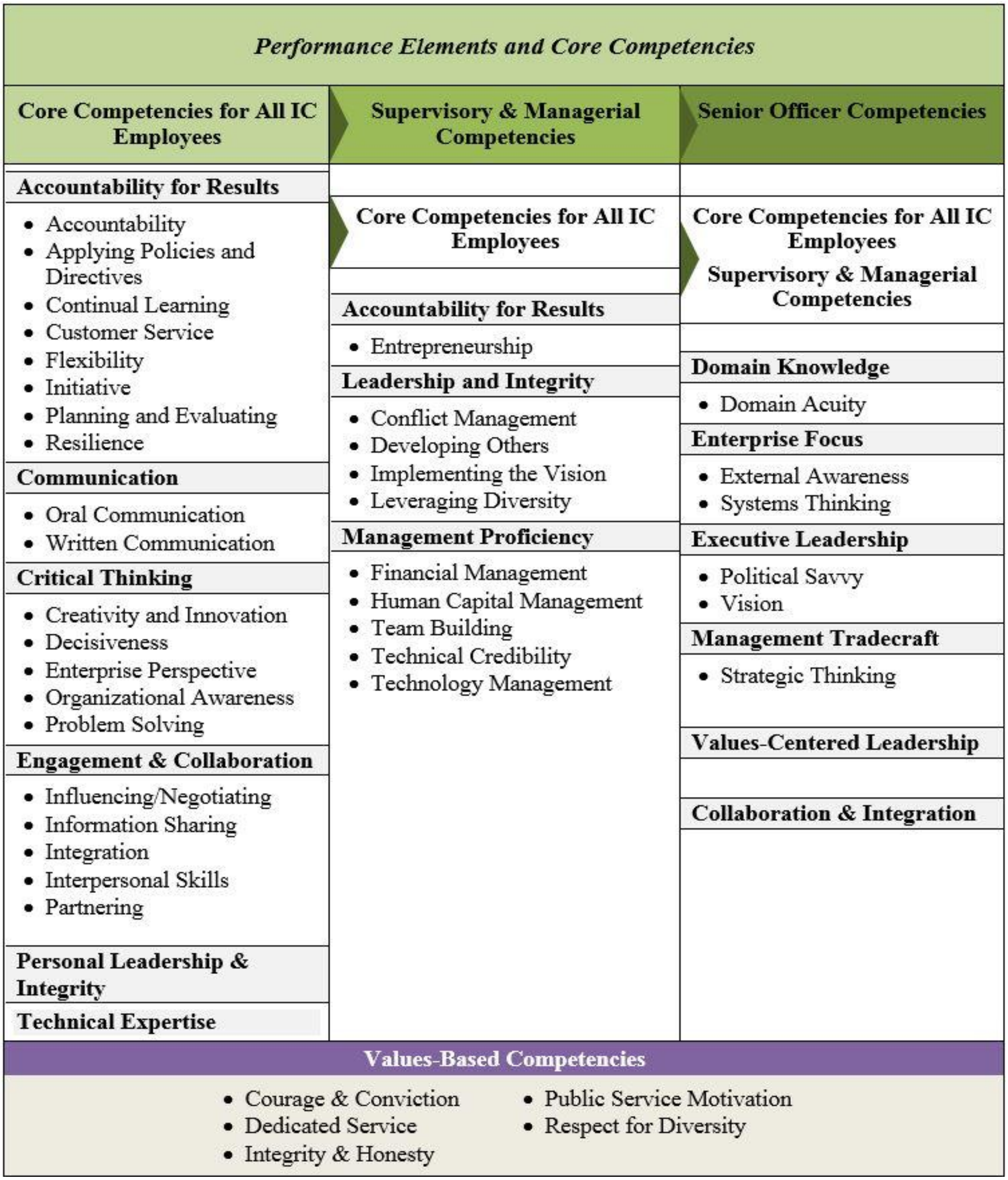
Technical Expertise Competencies

- Classification Management
- Counterintelligence
- Cyber Operations
- Data/Information Management
- Education and Training
- Evidence Gathering
- Exploitation Analysis
- Incident Response
- Information and Records Management
- Information Security
- Inquiry
- Inspection
- Intelligence Disciplines (INTs)
- Legal Theory and Practice
- Observation
- Personnel Security
- Policy Development
- Program Management Researching
- Security Awareness
- Security Program Management
- Synthesis
- Threat Analysis
- Vulnerabilities Assessment Management

Other Capabilities

- Tools and Methods

Table 3. IC Core Competencies



Performance Elements and Core Competencies

Core Competencies for All IC Employees	Supervisory & Managerial Competencies	Senior Officer Competencies
Accountability for Results - Accountability - Applying Policies and Directives - Continual Learning - Customer Service - Flexibility - Initiative - Planning and Evaluating - Resilience	**Core Competencies for All IC Employees**	**Core Competencies for All IC Employees** **Supervisory & Managerial Competencies**
Communication - Oral Communication - Written Communication	**Accountability for Results** - Entrepreneurship	**Domain Knowledge** - Domain Acuity
Critical Thinking - Creativity and Innovation - Decisiveness - Enterprise Perspective - Organizational Awareness - Problem Solving	**Leadership and Integrity** - Conflict Management - Developing Others - Implementing the Vision - Leveraging Diversity	**Enterprise Focus** - External Awareness - Systems Thinking
Engagement & Collaboration - Influencing/Negotiating - Information Sharing - Integration - Interpersonal Skills - Partnering	**Management Proficiency** - Financial Management - Human Capital Management - Team Building - Technical Credibility - Technology Management	**Executive Leadership** - Political Savvy - Vision
Personal Leadership & Integrity		**Management Tradecraft** - Strategic Thinking
Technical Expertise		**Values-Centered Leadership**
		Collaboration & Integration

Values-Based Competencies

- Courage & Conviction
- Dedicated Service
- Integrity & Honesty
- Public Service Motivation
- Respect for Diversity

Table 4. Core, Supervisory & Managerial, and Senior Officer Competencies Associated with Insider Threat KSAs

IC Core and Leadership Competencies	KSAs
Accountability Holds self and others accountable for measurable, high-quality, timely, and cost-effective results. Determines objectives, sets priorities, and delegates work. Accepts responsibility for mistakes. Complies with established control systems and rules.	• Knowledge of policy and procedures for identifying and reporting insider threat incidents. • Knowledge of procedures for reporting to mitigation authority or CI authorities. • Skill in evaluating and testing applicable Federal protocols and procedures covering insider threat methodologies. • Skill in making referrals/ recommendations to mitigation authorities.
Applying Policy and Directives Identifies, interprets, complies with and stays current on relevant regulations, guidelines, laws, and directives.	• Knowledge of Executive Order 13587, National Policy, and Minimum Standards. • Knowledge of relevant policies and protections for employees' civil liberties, civil rights, and privacy (e.g., whistleblower protections). • Skill in applying relevant laws, concepts, executive orders, regulations, directives, policies, and procedures to accomplish mission-based goals and objectives of the insider threat program.
Creativity and Innovation Develops new insights into situations; questions conventional approaches; encourages new ideas and innovations; designs and implements new or cutting edge programs/processes.	• Skill in developing and applying innovative improvements to plans, policies, and procedures.
Customer Service Anticipates and meets the needs of both internal and external customers. Delivers high-quality products and services; is committed to continuous improvement.	• Skill in producing innovative, all-source products for a broad set of customers, including DoD, IC, Security, Law Enforcement, and other government agencies.
Decisiveness Makes well-informed, effective, and timely decisions, even when data are limited or solutions produce unpleasant consequences; perceives the impact and implications of decisions.	• Skill in analyzing multiple data points to determine the best response (i.e., exoneration, internal review, or external referral). • Skill in making effective and timely decisions with limited information.
External Awareness Understands and keeps up-to-date on local, national, and international policies and trends that affect the organization and shape stakeholders' views; is aware of the organization's impact on the external environment.	• Knowledge of emerging issues relevant to U.S. national security.
Flexibility Is open to change and new information; rapidly adapts to new information, changing conditions, or unexpected obstacles.	• Ability to remain open to change and new information. • Skill in recognizing and incorporating new information.

IC Core and Leadership Competencies	KSAs
Influencing/Negotiating Persuades others, builds consensus through give and take, and gains cooperation from others to obtain information and accomplish goals.	• Skill in persuading others of the importance of the insider threat program.
Information Sharing Shares information, as appropriate, with customers, colleagues, and others. Ensures colleagues receive organizational information and recognizes the responsibility and takes action to provide information within the IC, to other federal, state and local law enforcement or authorities, the private sector, and/or foreign partners, as appropriate.	• Knowledge of guidelines, procedures, and approaches that support information sharing. • Skill in providing technical guidance to program stakeholders on insider threat requirements.
Integration Searches for opportunities to collaborate and actively promotes collaboration on work products and across work domains to enhance the quality of results.	• Skill in collaborating with other insider threat programs to review relevant information. • Skill in coordinating plan development and implementation with other program offices and organizations (e.g., CI, OPSEC, Law Enforcement). • Skill in leveraging opportunities to collaborate with other mission areas or agencies.
Oral Communication Makes clear and convincing oral presentations. Listens effectively; clarifies information as needed.	• Skill in presenting and justifying recommendations to various levels of officials. • Skill in presenting briefings and training.
Partnering Develops networks and builds alliances; collaborates across boundaries to build strategic relationships and achieve common goals.	• Skill in developing collaborative, interagency relationships.
Planning and Evaluating Organizes work, sets priorities, and determines resource requirements; determines short- or long-term goals and strategies to achieve them; coordinates with other organizations or parts of the organization to accomplish goals; monitors progress and evaluates outcomes.	• Skill in evaluating and prioritizing insider threat information. • Skill in evaluating and prioritizing program resource needs. • Skill in monitoring progress and evaluating outcomes.
Problem Solving Identifies and analyzes problems; weighs relevance and accuracy of information; generates and evaluates alternative solutions; and makes recommendations.	• Ability to understand and draw inferences from incomplete data. • Skill in forming competing hypotheses, ranking alternatives for complex decisions, and creating decision-making criteria.

IC Core and Leadership Competencies	KSAs
Systems Thinking Understands how variables within a system interact with one another and change over time. Applies this understanding to solve complex problems and drive integration.	• Knowledge of the Intelligence, Security, Law Enforcement, and CI communities, including their capabilities and jurisdictions.
Team Building Inspires and fosters team commitment, spirit, pride, and trust. Facilitates cooperation and motivates team members to accomplish group goals.	• Skill in organizing and inspiring an insider threat team to accomplish program goals.
Technical Credibility Understands and appropriately applies principles, procedures, requirements, regulations, and policies related to specialized expertise.	• Knowledge of relevant insider threat concerns, issues, and challenges. • Knowledge of issues, behaviors, and motivators indicative of insider threat risk. • Knowledge of behavioral science's application to the insider threat program. • Knowledge of insider threat program best practices. • Knowledge of insider threat minimum standards for assessing program maturity. • Skill in evaluating reporting thresholds for insider threat.
Written Communication Writes in a clear, concise, organized, and convincing manner for the intended audience.	• Skill in developing complex written guidance and reports summarizing a variety of information and drawing appropriate conclusions. • Skill in editing analytic products or training materials. • Skill in communicating ideas clearly and concisely.

Table 5. Relevant Technical Expertise Competencies Associated with Insider Threat KSAs

IC Technical Expertise Competencies	KSAs
Classification Management Applies the requirements for classifying, marking, redacting, handling, transporting, and safeguarding protected (e.g., FOIA/Privacy Act) and/or classified information.	• Knowledge of applicable rules and regulations regarding the handling, distribution, filing, and storage of classified and unclassified materials.
Counterintelligence Gathers information and conducts activities to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.	• Knowledge of CI principles, methods, and functional services. • Knowledge of reporting requirements for CI issues. • Skill in identifying indicators, behaviors, and modus operandi associated with foreign intelligence entities.
Cyber Operations Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.	• Knowledge of user monitoring capabilities for automated information systems. • Knowledge of defensive measures in order to protect information, information systems, and networks from insider threats. • Skill in monitoring computer networks for anomalous or unauthorized activities.
Data/Information Management Formats, catalogs, and/or filters data and information to facilitate data access, integration, and interpretation.	• Knowledge of relevant databases to find, extract, store, and retrieve relevant information. • Knowledge of local and national intelligence information databases. • Skill in entering, updating, and organizing data in information systems/databases so that it can be accessed by self and others.
Education and Training Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.	• Knowledge of design principles for insider threat awareness training. • Skill in providing insider threat awareness training.
Evidence Gathering Develops sources and recovers evidence. Analyzes data to determine compliance with laws, regulations, and policies. Draws conclusions as appropriate.	• Skill in collecting and aggregating information from various sources to evaluate potential insider threat indicators.

IC Technical Expertise Competencies	KSAs
Exploitation Analysis Analyzes collected information to verify vulnerabilities and potential for exploitation.	• Knowledge of processes to assess risks to the agency's critical assets from malicious insiders. • Skill in analyzing collected information to identify vulnerabilities and potential for exploitation.
Incident Response Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.	• Ability to respond to crises or urgent situations in order to mitigate immediate and potential threats. • Skill in identifying and reporting insider threat incidents. • Skill in executing (or overseeing execution of) established processes and procedures for containing, mitigating, or addressing the impact of insider threat incidents. • Skill in conducting administrative inquiries of insider threat issues. • Skill in coordinating responses to insider threat incidents.
Information and Records Management Gathers, organizes, maintains, and manages release and disposal of records and other information in accordance with FOIA, Privacy Act, Records Retention Policies, and other applicable guidelines. Develops and maintains databases, catalogs, or other lists; uses automated systems to locate and track items.	• Knowledge of various dissemination mechanisms and systems.
Information Security Applies knowledge of policies, procedures, and requirements established under appropriate authorities to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security.	• Knowledge of the "need-to-know" criteria for insider threat.
Inquiry Applies techniques for gathering information necessary to make legal determinations, develops new sources of information where appropriate, analyzes facts, and frames allegations to determine compliance with laws, regulations, and policies. Determines scope, methodology, and criteria to accomplish investigations in accordance with investigative standards, investigative policy, and standard operating procedures.	• Knowledge of established administrative inquiry processes, procedures, and authorities. • Skill in conducting insider threat interviews.
Inspection Plans and conducts organizational evaluations to assess their effectiveness and efficiency in accomplishing the mission.	• Skill in conducting evaluations to assess effectiveness and efficiency in accomplishing the insider threat program mission.

IC Technical Expertise Competencies	KSAs
Intelligence Disciplines (INTs) Applies knowledge of concepts and terminology, policies and directives, organizational missions, and functions, with respect to intelligence capabilities.	• Skill in relating insider threat subject-matter or functional expertise to intelligence needs.
Legal Theory and Practice Demonstrates knowledge of legal theory, the interrelationships among the courts, Congress, the Executive Branch, laws, legal codes, practices, precedents, court procedures, executive orders, government organization/functions, and the democratic process.	• Knowledge of the legal requirements for insider threat personnel and programs.
Observation Detects sequences in behavior and notices/attends to others' verbal and non-verbal cues. Maintains awareness of physical surroundings and detects factors that may impact physical, personnel, and operational security.	• Skill in determining whether behavior patterns warrant either closer scrutiny or referral to an investigative or administrative entity.
Personnel Security Applies personnel security principles and methods to process initial clearances, periodic re-investigations, and clearance upgrades/downgrades and to complete the adjudication and appeals processes. Evaluates internal and external security clearance requests and ensures applicants' actions are consistent with regulatory requirements. Analyzes and reports on clearance and appeals findings to senior security officials and makes appropriate notifications.	• Knowledge of the adjudicative process. • Knowledge of the contents of Personnel Security Investigation reports of investigation and their utility to insider threat programs. • Knowledge of Personnel Security Investigation types and information gathered. • Knowledge of the personnel security and issues that may affect personnel security. • Knowledge of policies and regulations on foreign travel, reporting contact with foreign nationals, etc.
Policy Development Develops policy or advocates for changes in policy that will support new initiatives or required changes/enhancements.	• Skill in developing insider threat policies and procedures, and advocating for changes to support initiatives or enhancements.
Program Management Applies program management principles, techniques, services, and practices to effectively achieve domestic and international program goals and objectives. Identifies performance outcomes and establishes metrics to assess the impact (e.g., return on investment) of programs and initiatives.	• Knowledge of requirements for insider threat programs.

IC Technical Expertise Competencies	KSAs
Researching Identifies a need for and knows where or how to gather information. Obtains, evaluates, organizes, and maintains information.	• Skill conducting research and recognizing relevance of findings.
Security Awareness Understands policies, regulations, and procedures for securing government and contractor facilities to prevent unauthorized access to facilities and information. This may include assessing and mitigating technical and terrorist threats, and/or vulnerabilities.	• Knowledge of security and vulnerability points for physical security. • Skill in assessing and mitigating threats and/or vulnerabilities.
Security Program Management Manages information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources.	• Ability to assess the compliance of the insider threat program with relevant laws, directives, and policies. • Knowledge of the minimum standards for insider threat programs. • Knowledge of principles for establishing an insider threat analysis center or single-point program for insider threat. • Skill in coordinating execution of risk assessments to assess program protection effectiveness.
Synthesis Analyzes, interprets, and integrates data or other information; evaluates and prioritizes alternatives; and assesses similarities and differences in data to develop findings and conclusions.	• Knowledge of methods to gather, integrate, and analyze CI, security, IA, HR, LE, and other relevant information to respond to potential insider threat incidents. • Skill in reviewing and assimilating information from multiple sources to uncover notable patterns in behavior. • Skill in assessing trends, patterns, and relationships from multiple sources to draw relevant conclusions. • Skill in interpreting data to determine insider threat indicators and/or anomalous activities. • Skill in using data visualization tools and techniques.
Threat Analysis Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence agencies; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.	• Knowledge of potential criminal behaviors and activities. • Skill in conducting assessments to systematically evaluate risks.
Vulnerabilities Assessment and Management Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations or enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.	• Knowledge of factors impacting an agency's insider threat risk. • Skill in leveraging threat assessment results. • Skill in executing (or overseeing execution of) established processes and procedures for containing, mitigating, or addressing the impact of insider threat incidents. • Skill in conducting loss, threat, risk, and vulnerability analyses.

Table 6. Other Insider Threat-related Capabilities with KSAs

Other Capabilities	KSAs
Tools and Methods Applies tools and methods to substantive discipline, domain, or area of work. Adapts existing tools and/or methods or employs new methodological approaches required for substantive discipline, domain, or area of work. A tool is a physical or virtual device (e.g., Analyst Notebook, Intelink, data extraction tools) used to perform work rather than something that is studied, exploited, or targeted. A method is a structured and repeatable process for carrying out work (e.g., analysis of competing hypotheses, modeling, and simulation).	• Knowledge of the scope, availability, and requirements of techniques and tools for collecting, analyzing, visualizing, and reporting on complex information. • Skill in using insider threat tools.