NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

National Counterintelligence Strategy of the United States of America 2016

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2015		**00-00-2015 to 00-00-2015**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
National Counterintelligence Strategy of the United States of America 2016	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Director of National Intelligence (ODNI),National Counterintelligence and Security Center ,Washington,DC,20511**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**20**	


E PLURIBUS UNUM

THE WHITE HOUSE

WASHINGTON

Today, the United States faces a daunting counterintelligence threat that seeks to undermine our economic strength, steal our most sensitive information, and weaken our defenses. As we have throughout history, we must rely on a strong counterintelligence regimen that detects, deters, and disrupts the threats of today while preparing for the challenges of tomorrow.

Foreign intelligence entities, as well as terrorist groups and non-state actors, use human and technical means, both overtly and covertly, to steal U.S. national security information. We know they are actively seeking to acquire data on a range of sensitive topics of vital importance to our security -- from advanced weapons systems and intelligence capabilities, to proprietary information from U.S. businesses and institutions in the fields of energy, finance, defense, and dual-use technology.

We also know that cyber tools and new technologies are giving our adversaries new ways to steal valuable data from the United States Government, academic institutions, and businesses -- oftentimes from the safety of a computer thousands of miles away. As the recent cyber intrusion against the Office of Personnel Management illustrated, even Federal agencies that hold sensitive but not classified data are at increased risk of being targeted by foreign adversaries. The expanding and interconnected nature of espionage threats demands a whole-of-government response to safeguard our most valuable security and economic information.

The *National Counterintelligence Strategy of the United States of America 2016* sets forth a coordinated plan to detect, deter, and disrupt foreign threats by strengthening bonds and information sharing among government, academic institutions, and the private sector. It elevates the focus on countering cyberespionage and provides guidance to U.S. entities to unify efforts at home and abroad against today's threats while preparing for those of tomorrow.


E PLURIBUS UNUM

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
NATIONAL COUNTERINTELLIGENCE EXECUTIVE
WASHINGTON, DC 20511

This *National Counterintelligence Strategy of the United States of America 2016 (Strategy)* represents an evolution in our approach to a whole-of-government awareness of and response to foreign intelligence entity (FIE) threats. In recent decades, the United States Government has made extraordinary strides adapting to changing fiscal, technological, and cultural environments. However, the efforts to modernize and adapt have likewise provided opportunities for FIEs to expand their scope of collection and operations against the U.S. Government.

The United States remains vulnerable if it is only capable of recognizing the threat. Recognition must be followed by means to counter such threats. Fully integrating counterintelligence (CI) and security into our business practices—from information technology and acquisition to personnel decisions—is essential to preserving our national security. We must leverage the CI and security disciplines to create mission synergies and extend these synergies into the realm of cyberspace. We must work with our information assurance professionals to defend our networks from FIEs attempting to steal or compromise our sensitive data, information, and assets. We must bolster our collection and analytic efforts, improve targeting to disrupt the operations of FIEs, and foster widespread awareness and application of CI. By doing so, we will expand the reach and improve the effectiveness of CI across the U.S. Government.

My office is committed to working with leaders across the U.S. Government and private sector to drive reforms needed to protect our national security and mitigate the threats posed by FIEs. As leaders, it is our collective responsibility to be ahead of the threat. Each senior leader has the opportunity to be a change agent, to transform business practices and shape the workforce to support and protect our most sensitive information and assets. This *Strategy* is a roadmap to unify and modernize our efforts; through its implementation, we will leverage the talents of the entire U.S. Government to protect our nation's most sensitive information and assets.

William R. Evanina


E PLURIBUS UNUM

Purpose

The *National Counterintelligence Strategy of the United States of America 2016 (Strategy)* was developed in accordance with the Counterintelligence Enhancement Act of 2002 (Pub.L. No. 107-306, 116 Stat. 2383 (as amended) codified at 50 U.S.C. sec. 3383(d)(2)). The *Strategy* sets forth how the United States (U.S.) Government will identify, detect, exploit, disrupt, and neutralize foreign intelligence entity (FIE) threats. It provides guidance for the counterintelligence (CI) programs and activities of the U.S. Government intended to mitigate such threats.

Each U.S. Government department and agency has a role in implementing this *Strategy* in the context of its own mission and through application of its unique responsibilities and authorities. Nothing in this *Strategy* shall be construed as authorization of any department or agency to conduct CI activities not otherwise authorized under statute, executive order, or any other applicable law, policy, or regulation.

Strategic Environment

The United States is confronted with an array of diverse threats and challenges from FIE activities. Our adversaries include not only foreign intelligence services and their surrogates but also terrorists, cyber intruders, malicious insiders, transnational criminal organizations, and international industrial competitors with known or suspected ties to these entities. Many use sophisticated overt, covert, and clandestine methods to compromise our national security.

Just as the nature, scope, and volume of our protected information and other vulnerable assets have evolved, so too has the threat environment. Technological advances have enabled our adversaries to both broaden and tailor their approach to subvert our defensive measures, harm and penetrate our information systems, steal sensitive data, and otherwise degrade our instruments of national power.

Strategic Response

The current and emerging CI challenges facing the U.S. require an integrated, whole-of-government response. Successfully countering threats from FIEs requires the U.S., both public and private sectors, to recognize the threat environment and implement appropriate countermeasures. The mission of countering FIEs is essential to preserving U.S. decision-making confidence and the critical information, technologies, infrastructure, and other assets that underpin our nation's security and prosperity. Understanding the threats and responding in an integrated fashion are imperative to the successful implementation of this *Strategy*.

Force Multipliers

The unfailing application of proactive, effective security capabilities is crucial to protect sensitive U.S. information and assets from foreign adversaries. While the authorities that govern CI and security and the programs they drive are distinct, their respective actions must be synchronized and coordinated to achieve results. CI and security are interdependent and mutually supportive disciplines with shared objectives and responsibilities associated with the protection of sensitive information and assets. This *Strategy* acknowledges the critical role of security programs in contributing to the integrity of our CI efforts.

Moreover, defending the increasingly complex networks and technology that house and process our sensitive information against sophisticated 21st century threats requires a seamless and well-coordinated four-pronged defensive approach comprising CI, security, information assurance (IA), and cybersecurity professionals working together as a team. Essential to this *Strategy* is leveraging security and CI disciplines to create mission synergies and extending these synergies into the realm of cyberspace. CI, security, and IA combine in a multidisciplinary approach to provide a more stable network defense posture.

This *Strategy* puts forth both mission and enabling objectives to address the full range of capabilities needed to counter the diverse threats to our nation's sensitive information and assets. The five mission objectives outline key activities required to identify, detect, exploit, disrupt, and neutralize FIE and insider threats and to safeguard our national assets, including cyberspace. The two enabling objectives provide the foundation for the mission objectives' success by highlighting the need for these activities to be undertaken as part of an effective, responsible, and collaborative effort. Implemented together, the mission and enabling objectives create a CI posture capable of meeting 21st century threats.

MISSION OBJECTIVE 1

Deepen our understanding of foreign intelligence entities' plans, intentions, capabilities, tradecraft, and operations targeting U.S. national interests and sensitive information and assets

The United States faces enduring and emerging threats from FIEs that target our sensitive information and assets or otherwise jeopardize U.S. national interests. These threats continue to evolve in scope and complexity as FIE capabilities and activities become increasingly diverse and technically sophisticated. To meet this challenge, the U.S. Government must continue to evolve its CI programs and activities to improve our understanding of the full scope of current and emerging FIE threats, drive decision-making, and support U.S. national security goals.

In accordance with their existing authorities, mission, roles, and responsibilities, departments and agencies will:

- Conduct and support collection, investigative, and operational activities that yield intelligence on FIEs' strategic objectives and collection priorities;
- Conduct and support collection, investigative, and operational activities that yield intelligence on FIEs' plans, intentions, capabilities, and activities;
- Penetrate and pursue FIEs in order to holistically understand FIE threats;
- Produce timely, forward leaning all-source analytic products on FIE capabilities and intentions that provide warning and identify key changes, trends, and events;
- Disseminate CI-relevant information obtained during the course of investigations and operations;
- Pursue joint collection and analysis opportunities to expand and enrich reporting and production on priority FIE targets;
- Develop and implement efforts to anticipate, identify, and warn of emerging FIE threats; and
- Conduct and support collection, investigative, and operational activities that identify technical capabilities and threats.

Successful implementation of these actions will yield actionable intelligence on FIE threats to U.S. national security, including joint products that provide policymakers relevant, insightful, and credible intelligence to close the highest priority knowledge gaps. It will also provide warnings to U.S. Government departments and agencies and private sector partners of specific FIE threats to their information and assets.

MISSION OBJECTIVE 2

Disrupt foreign intelligence entities' capabilities, plans, and operations that threaten U.S. national interests and sensitive information and assets

FIEs pursue sophisticated measures to disrupt U.S. plans, policies, and processes and undermine U.S. national interests. All of these activities threaten the advancement of U.S. national security goals. The U.S. Government must employ coordinated offensive and defensive CI activities aligned to U.S. national security requirements to effectively disrupt FIE advances. By guarding against FIE threats while taking proactive steps to respond to them, we seek to counter, disrupt, and defeat activities inimical to the interests of the United States.

In accordance with their existing authorities, mission, roles, and responsibilities, departments and agencies will:

- Conduct and support, as appropriate, collection, investigative, and operational activities that identify and disrupt efforts to penetrate or influence the U.S. Government or otherwise harm U.S. interests;
- Conduct and support, as appropriate, CI operations that corrupt the integrity of foreign adversaries' intelligence cycles;
- Conduct and support, as appropriate, collection, investigative, and operational activities that counter, exploit, or otherwise defeat FIEs' activities; and
- Promote collaborative and integrated efforts to counter FIE threats in order to optimize government-wide capabilities and amplify individual lines of effort.

Successful implementation of these actions will result in disruptions of FIE intelligence activities. A measureable decline in the level of risk to sensitive information and assets, as determined and mitigated through periodic risk assessments, should occur. Information gleaned from these actions should form the basis of a coordinated, agile, and highly responsive process for identifying and prioritizing FIE threats and intelligence gaps. This process will provide greater fidelity in characterizing and countering FIE threats.

MISSION OBJECTIVE 3

Detect, deter, and mitigate threats from insiders with access to sensitive information and assets

The U.S. Government continues to face threats from trusted insiders who compromise our intelligence sources and methods. These insiders range from those who are driven by personal ideology or directed by foreign governments to those whose unintentional actions jeopardize national security. Recent unauthorized public disclosures by trusted insiders have damaged international relationships, compromised intelligence sources, and prompted our adversaries to change their behavior, making it more difficult to understand their intentions.

The early detection of insider threats is essential to protecting our sensitive information and assets. Information and data gathered from multiple sources are integral components of a department's or agency's ability to detect and mitigate threats from malicious insiders. We must also recognize that the most effective safeguard against insider threats is a knowledgeable, trusted workforce which is confident that their privacy and civil liberties are respected. Employees are the caretakers of our most sensitive information and resources, and they must be individually invested in the imperative to protect it.

In accordance with their existing authorities, mission, roles, and responsibilities, departments and agencies will:

- Integrate and analyze relevant CI data and work with enterprise insider threat programs to use a whole-person, whole-of-career concept to identify and continuously evaluate anomalous behavior;

- Review insider threat anomalies for FIE nexuses;
- Analyze FIE activities to discern patterns of behavior potentially indicative of an insider threat;
- Advocate for and influence the implementation of automated records-check methodologies to identify relevant CI information;
- Ensure CI equities are incorporated into a risk-based approach to insider threat detection techniques;
- Strengthen CI and insider threat awareness among the workforce to enhance and drive vigilance and consciousness across the U.S. Government;
- Enable network and system monitoring and ensure triggers are evaluated and cross-checked against other data sources to enhance detection and analysis of possible anomalous behavior; and
- Advocate for participation in enterprise audit programs to prevent unauthorized activity and facilitate a secure information infrastructure.

Successful implementation of these initiatives will best posture departments and agencies for early detection of anomalous behavior and improve the identification, prevention, and mitigation of uncharacteristic employee conduct or harmful insider threat activities. Enhanced insider threat and CI awareness across the U.S. Government will improve our ability to identify suspicious activities, identify FIE attempts to collect information or recruit employees, and instill a sense of urgency to report anomalous behaviors or activities to security and counterintelligence professionals. Better management of shared information will limit the availability of and access to classified and potentially sensitive information. Early detection and mitigation is critical for a successful insider threat program to minimize the damage caused by employees who intentionally or unintentionally compromise our information and systems, and, in more serious cases, to neutralize FIE attempts to recruit employees.

MISSION OBJECTIVE 4

Safeguard sensitive information and assets from foreign intelligence entities' theft, manipulation, or exploitation

Foreign intelligence entities threaten U.S. national security as they relentlessly seek access to sensitive U.S. information and assets that will provide them with an economic, military, or technological edge. At the same time, vulnerabilities in global supply chains increase the potential for adversaries to exploit, deny, or damage U.S. assets and services. In the aggregate, such activities may undercut U.S. economic and military security and affect a wide variety of national security-related activities. The threat extends beyond the U.S. Government—U.S. companies and research establishments are target-rich environments for FIEs. To effectively protect our information and assets, the U.S. Government must engage stakeholders across the public and private sectors to ensure a common understanding of, and response to, FIE activities.

In accordance with their existing authorities, mission, roles, and responsibilities, departments and agencies will:

- Employ programs and activities to protect the integrity of the U.S. intelligence system and ensure the continuing performance of national essential functions;
- Use programs and activities to defend our critical infrastructure; critical and emerging technologies; and research, development, and acquisition programs from FIE collection or illicit acquisition;
- Implement programs and activities that facilitate secure information sharing and collaboration with foreign partners, vendors, researchers, and visitors while protecting sensitive information and assets from FIE theft, manipulation, or exploitation;
- Identify vulnerabilities and threats to private sector entities conducting sensitive U.S. Government-sponsored research, development, and acquisition programs;
- Integrate CI and security process into supply chain operations to secure the supply chain from exploitation and reduce its vulnerability to disruption;
- Expand partnerships with law enforcement agencies responsible for enforcing export control rules to identify unauthorized exports and take aggressive criminal and administrative enforcement actions against FIEs;

- Conduct risk assessments to identify and mitigate FIE threats to product development, acquisition, implementation, and maintenance cycles; and
- Coordinate efforts to safeguard sensitive information and assets across the U.S. Government.

Successful implementation of these actions will require an increase in U.S. Government and private sector partners sharing threat information; an increase in the education and awareness of employees on FIE interest in our sensitive information and assets; and an increase in the number of risk assessments conducted on organizations researching, manufacturing, or procuring sensitive technologies and assets. Other indicators of success include improvements in our application of protective measures countering FIE theft, manipulation, or exploitation throughout all phases of the supply chain.

MISSION OBJECTIVE 5

Identify and counter foreign intelligence entities' cyber activities that attempt to disrupt, exploit, or steal sensitive information, to include personally identifiable information, from U.S. networks

FIEs continue to use computer network operations to exfiltrate sensitive data, information, and assets from the U.S. Government and the private sector, as observed in several recent data breaches. The loss of sensitive data, information, and assets through computer network operations conducted by or on behalf of FIEs has the potential to cause significant economic, technological, scientific, and national security harm and introduce counterintelligence and cybersecurity

vulnerabilities. In addition to providing FIEs with sensitive U.S information, network compromises may increase options for disrupting communications networks and critical infrastructure systems. Technological advances have accelerated the speed at which information moves, challenging our capability to protect sensitive information and assets. Because of these challenges, a robust capability to defend against adversarial computer network operations must be tightly woven into U.S. Government CI and security programs, including the expansion of outreach programs with private sector partners.

In accordance with their existing authorities, mission, roles, and responsibilities, and in response to recent cyberespionage breaches, departments and agencies will:

- Expand support to cyber effects operations;
- Pursue programs and activities that enhance understanding of FIE cyber intentions, capabilities, and operations affecting U.S. networks;
- Advance attribution capabilities to support disruption of cyber attacks and exploitation linked to FIEs;
- Enhance the relationship between CI elements, security, and IT to ensure personally identifiable information, and other sensitive information and assets of interests to FIEs is protected;
- Pursue programs and activities that counter FIE cyber operations directed against sensitive U.S. information; and
- Leverage expertise across the CI, security, and information technology mission sets to identify and assess stolen content, analyze and mitigate risks, and define protection requirements.

Successful implementation of these actions will enhance a department's or agency's ability to analyze incidents and attribute suspicious network behavior to FIE activities. Other indicators of success include a continued increase in threat information-sharing across all sectors and collaboration on mitigation strategies.

ENABLING OBJECTIVE 1

Strengthen secure collaboration, responsible information sharing and safeguarding, and effective partnerships

FIEs target the U.S. Government and our private sector and international partners to obtain not only classified, but also sensitive information and assets. As a result, a persistent and growing need exists to collaborate and share FIE threat, warning, and awareness information across the entire U.S. Government and with the private sector and international partners. At the same time, we must ensure personnel engaged in these information discovery and retrieval efforts are mindful of the safeguards necessary to protect sensitive information and assets.

Secure collaboration, responsible information sharing, and effective partnerships are vital in detecting, identifying, exploiting, and neutralizing FIE efforts to compromise and degrade U.S. national and economic security.

In accordance with their existing authorities, mission, roles, and responsibilities, departments and agencies will:

- Drive responsible and secure information sharing to maximize unity of effort in identifying, exploiting, and neutralizing FIE threats and to inform decision making;

- Enhance synchronization of CI programs and activities, including the conduct of joint investigations and operations;
- Expand partnerships and share threat information across U.S. Government agencies and with key public and private sectors and international partners to establish a common understanding of FIE threats and promote coordinated mitigation approaches;
- Develop and deliver credible education and awareness programs that equip the U.S. Government workforce and public and private sector partners to identify threats and report CI concerns;
- Share information on FIE technical activities and capabilities across U.S. Government agencies and with key public and private sectors and international partners to address pervasive threats and vulnerabilities; and
- Share information on lessons learned and best practices with across U.S. Government agencies and with key public and private sectors and international partners to improve our processes for reporting, analyzing, investigating, and remediating incidents.

Successful implementation of these actions will yield an increase in information sharing to stem the damage caused by FIE activities. It should also improve the access of departments and agencies to reporting and production on common threats to U.S. national and economic security. In addition, it should result in an increase in CI training programs for U.S. Government personnel and in the percent of personnel trained.

ENABLING OBJECTIVE 2

Strengthen the nation's programs to counter threats from foreign intelligence entities

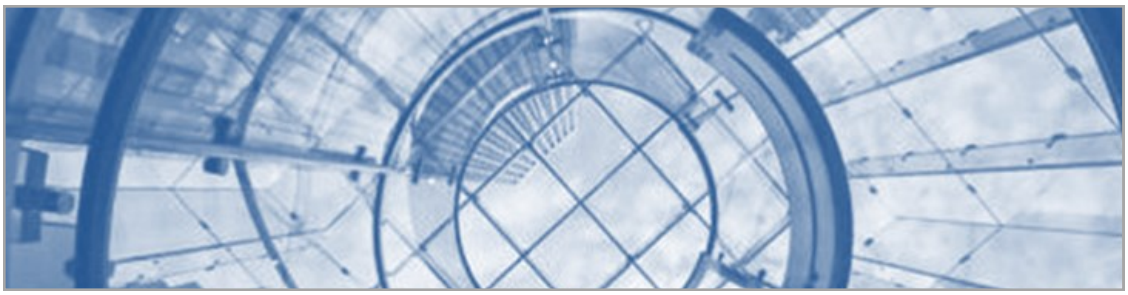
The U.S. Government's CI programs vary significantly in breadth and are calibrated to the unique mission requirements and organizational capabilities of each department and agency. Regardless of individual program complexities and proficiencies, the U.S. Government must strengthen its CI programs and processes to adapt to the complexity of FIE and insider threats. U.S. Government departments and agencies must plan and fund programs and activities to ensure that CI practitioners have the proper tools and resources to execute their responsibilities. At the same time, the tasks and activities that make up our CI programs must be continuously reviewed, renewed, and refined to ensure that the CI enterprise remains relevant, responsive, and effective.

In accordance with their existing authorities, mission, roles, and responsibilities, departments and agencies will:

- Promote well-reasoned and continuous integration of CI and FIE threat awareness into the execution of programs and activities across the U.S. Government;
- Provide continuous learning and professional development programs to increase professional skills and abilities in countering FIE;
- Develop strategies, policies, and oversight mechanisms to guide the execution of CI functions;
- Use risk assessment information to strengthen programs countering FIE threats; and

- Implement processes to track the effectiveness of CI efforts against stated national objectives and outcomes.

Successful implementation of these actions will result in an increase in the establishment, participation, and maturity of new and existing programs to counter FIE threats, as determined by formal evaluations. It should also result in greater awareness of and access to professional development opportunities to enhance the skills and proficiency of professionals responsible for protecting sensitive information and assets within departments and agencies. Additionally, it should result in an expanded use of existing and development, as needed, of new CI authorities, policies, and oversight mechanisms across the U.S. Government.



Conclusion

Countering FIE threats is a core obligation across the U.S. Government and should be reflected in the attitudes and daily behavior of the entire workforce. The U.S. Government must integrate CI principles and practices with business processes and workflows; mission-critical acquisitions; personnel, physical, and information security programs; and information assurance policies and procedures.

Our national security hinges on our ability to break down the wall separating CI from other core functions and transcend a paradigm that countering the FIE threats and protecting sensitive information and assets are the realm solely of CI and security professionals. While CI has traditionally operated as a stand-alone discipline, some U.S Government departments and agencies have made notable progress in recent years in integrating CI programs with security, insider threat, human resources, information assurance, budget, and other organizational functions. As the FIE threats facing us today continue to evolve, we must accelerate this integration and widen CI practices across the U.S. Government.

Achieving the mission and enabling objectives in this *National Counterintelligence Strategy of the United States of America 2016* is paramount to increasing our ability to counter FIE threats. Department and agency executives must become the change agents in implementing these mission and enabling objectives. Integrating our collective CI efforts and broadening their reach throughout the U.S. Government is vital to our success. By extending CI practices both across and within departments and agencies, we will exponentially strengthen the protection of the sensitive information and assets that underpin our national security.

Glossary

Terms not specifically cited were developed and defined in coordination with subject matter experts for use in this Strategy.

Acquisition – Acquiring by contract with appropriated funds of supplies or services (including construction) by and for the use of the Federal Government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contract, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract. – *Federal Acquisition Regulations, as of 29 January 2013*

Counterintelligence – Information gathered and activities conducted 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. – *Executive Order 12333, as amended, United States Intelligence Activities*

Counterintelligence Programs – Capabilities and activities established within an organization for the purposes of identifying, deceiving, exploiting, disrupting, or protecting against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign intelligence entities. – *Intelligence Community Directive 750, Counterintelligence Programs*

Counterintelligence Risk Assessment – An assessment that examines threat information and identifies organizational vulnerabilities to make an informed determination about the likelihood and consequence of the loss or compromise of sensitive information and assets to foreign intelligence entities.

Cyber Effect – The manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. – *Presidential Policy Directive/PPD-20, U.S. Cyber Operations*

Cyberspace – The interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer, information or communications systems, networks, and embedded processors and controllers. – *Presidential Policy Directive/ PPD-20, U.S. Cyber Operations Policy*

Espionage – Intelligence activity directed toward the acquisition of intelligence through clandestine methods. – *National Security Council Intelligence Directive No.5, U.S. Espionage and Counterintelligence Activities Abroad*

Foreign Intelligence Entity (FIE) – Known or suspected foreign state or non-state organizations or persons that conduct intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists. – *Intelligence Community Directive 750, Counterintelligence Programs*

Information Technology (IT) – Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which 1) requires the use of such equipment; or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. – *Committee on National Security Systems Instruction No. 4009, National Information Assurance Glossary*

Insider – Any person with authorized access to any U.S. Government resource, to include personnel, facilities, information, equipment, networks, or systems. – *National Insider Threat Policy, 2012*

Insider Threat – The threat that an insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the U.S. through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities. – *National Insider Threat Policy, 2012*

Intelligence Community –The term "intelligence community" includes the following: (A) The Office of the Director of National Intelligence. (B) The Central Intelligence Agency. (C) The National Security Agency. (D) The Defense Intelligence Agency. (E) The National Geospatial-Intelligence Agency. (F) The National Reconnaissance Office. (G) Other offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs. (H) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy. (I) The Bureau of Intelligence and Research of the Department of State. (J) The Office of Intelligence and Analysis of the Department of the Treasury. (K) The Office of Intelligence and Analysis of the Department of Homeland Security. (I) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director National Intelligence and the head of the department or agency concerned, as an element of the intelligence community. – *National Security Act of 1947, 50 U.S.C. sec. 3003(4)*

Personally Identifiable Information (PII) – Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. – *Office of Management and Budget Memorandum 07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information*

Private Sector – For-profit businesses, non-profits, and non-governmental organizations (including but not limited to think tanks, business trade associations, and academia) not owned or operated by the government.

Public Sector – Federal, state, territorial, tribal, and local governments that provide basic goods and services that either are not or cannot be provided by the private sector.

Sensitive Information and Assets – Refers to: 1) Information classified pursuant to Executive Order 13526, Classified National Security Information, including such information provided to industry in accordance with EO 12829, National Industrial Security Program, and EO 13549, Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities; 2) Critical infrastructure, as defined in EO 13636, Improving Critical Infrastructure Cybersecurity, which includes systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters; and 3) Controlled unclassified information, as determined by department and agency heads in accordance with EO 13556, Controlled Unclassified Information.

Supply Chain – A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to customers. – *Committee on National Security Systems Instruction No. 4009, National Information Assurance Glossary*


E PLURIBUS UNUM