NCSC | Know the Risk Raise your Shield

Office of the Director of National Intelligence
National Counterintelligence and Security Center

COUNTERING FOREIGN INTELLIGENCE THREATS

IMPLEMENTATION AND BEST PRACTICES GUIDE

For more information, visit www.NCSC.gov and follow us on Twitter @NCSCgov

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
WASHINGTON, DC 20511

U.S. government departments and agencies are custodians of sensitive information, assets and technologies—both classified and unclassified—that are vital to our national and economic security and are routinely targeted by foreign intelligence entities (FIE). Though robust policies and programs exist today for protecting classified information and systems, significant gaps remain in the safeguarding of sensitive information across the executive branch, particularly among organizations outside the Intelligence Community and Department of Defense. The National Counterintelligence and Security Center (NCSC) is seeking to raise awareness across the federal workforce about foreign intelligence threats and push forward the necessary policy guidance, tools, and resources for organizations to build and strengthen capabilities for countering those threats.

Departments and agencies are already required to protect multiple forms of sensitive information, including trade secrets, critical infrastructure data, personally identifiable information, and much more. The *National Counterintelligence (CI) Strategy of the United States of America 2016* directs departments and agencies to safeguard these assets specifically from FIE espionage efforts, and to build and strengthen programs to counter those efforts.

NCSC published this *Countering Foreign Intelligence Threats: Implementation and Best Practices Guide* to help departments and agencies strengthen their protective programs. The *Guide* provides tools and procedures that can help departments and agencies to address a central objective of the *CI Strategy*—to reduce the risk of FIE penetration. In using the *Guide*, each organization should tailor protective approaches considering their unique mission needs.

The NCSC stands ready to assist organizations by providing threat warnings and assessments, and sharing additional best practices, methodologies, and training tools. I am committed to working with leaders across the government to protect our national security and mitigate FIE-driven risk, and I look forward to working with you to build strong and resilient protective programs.

William R. Evanina

Countering FIE Threats: Best Practices

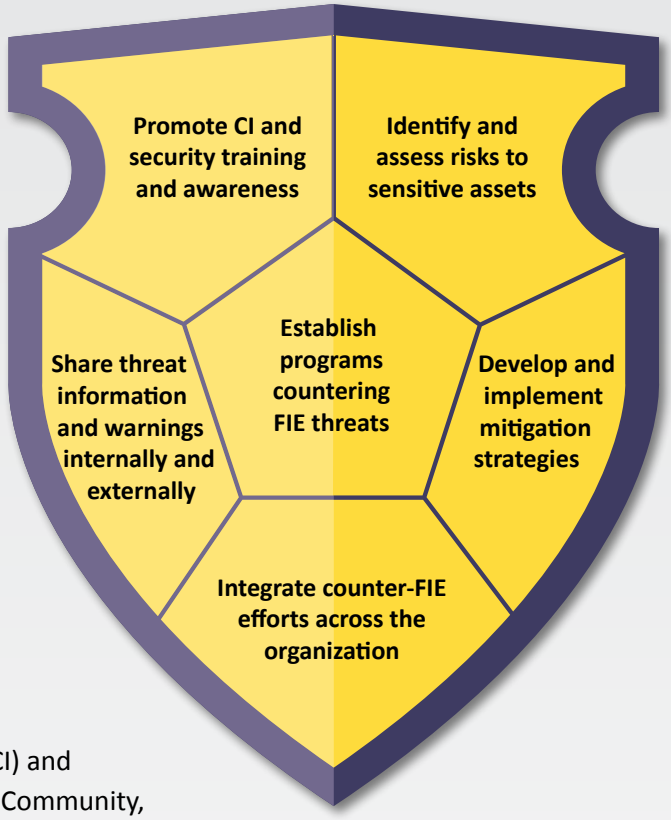
Know the Risk
Raise your Shield

Effective programs to counter foreign intelligence entity (FIE) threats are focused on three overarching outcomes:

1. Identification of foreign intelligence threats and sharing of threat information

2. Safeguarding of sensitive information, assets, and activities

3. Prevention and detection of insider threats

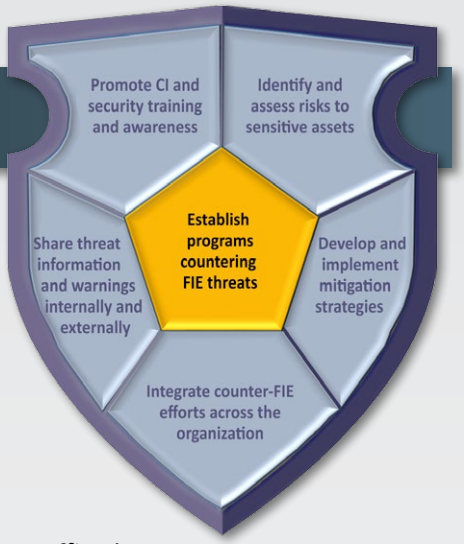


The best practices detailed in this *Guide*, from identifying and assessing risks to promoting training and awareness, are complementary program components that, when employed together, can effectively shield your organization from FIE threats.

The National Counterintelligence and Security Center (NCSC) is charged with leading and supporting the counterintelligence (CI) and security activities of the U.S. government, the U.S. Intelligence Community, and U.S. private sector entities that are at risk of intelligence collection, penetration, or attack by foreign adversaries and malicious insiders. The capabilities and activities described in this *Guide* are exemplars of program components delineated as requirements in numerous strategies, policies, and guidelines. This *Guide* is a living document and will be updated to reflect improved and innovative ways to achieve the above outcomes. In addition, organization-specific capabilities and activities may be defined and implemented to ensure unique needs are met. Finally, nothing in this document shall be construed as authorization for any organization to conduct activities not otherwise authorized under statute, executive order, or other applicable law, policy, or regulation, nor does this document obviate an organization's responsibility to conduct activities that are otherwise mandated, directed, or recommended for execution under the same.

Best Practice #1

Establish Programs Countering FIE Threats



Purpose and Description:
A program provides a formal organizational construct for countering FIE threats. It should be positioned so that the effort to counter threats to sensitive information and assets is given comparable priority and resources as other parts of the organization and is given consideration during activities such as budget formulation and allocation discussions, staffing determinations, strategic planning, and other leadership conversations/decisions.

Recommendation: Heads of departments and agencies should designate a senior official within their organization who shall be responsible for countering threats from FIEs.

☐ **Action:** Designate a senior official responsible for implementing and overseeing the program for countering threats from FIEs.

Note: The designated official should have direct access to the head of the organization as well as to the organization's security, CI, acquisition/procurement, and information technology (IT) senior leadership. Additionally, the selected official should work closely with the senior official designated under the requirements of the *White House Memorandum on National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs* for leading efforts to counter threats to the agency from malicious insiders.

Recommendation: The designated senior official should lead the development of policies, procedures, or guidelines designed to implement a program within his or her organization for countering FIE threats.

☐ **Action:** In consultation with program managers, develop and implement policies, procedures, and guidelines to not only safeguard the organization's sensitive assets, but also mitigate vulnerabilities to any known, specific FIE threats to those assets.

☐ **Action:** Identify resource needs, develop and justify the program's budget, and seek assistance from NCSC to provide advocacy, where necessary. The senior official should also ensure that training and professional development opportunities are made available to personnel directly responsible for CI and security program elements.

☐ **Option:** Organizations may establish additional requirements of their own, provided they are consistent with applicable laws, presidential directives, and other authorities.

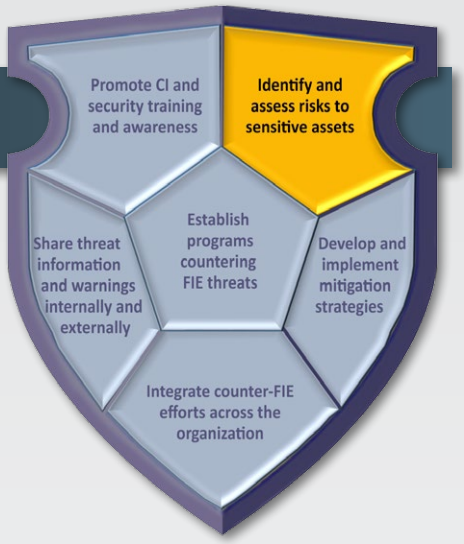
Recommendation: The designated senior official should build interdisciplinary partnerships among elements of the organization, including CI, security, information assurance (IA), chief information officer (CIO), human resources (HR), and acquisition/procurement.

☐ **Action:** Develop relationships inside and outside the agency and communicate the importance of understanding and countering the FIE threat.

Note: These partnerships should result in effective sharing of information about FIE threats and organizational vulnerabilities associated with sensitive information, assets, and activities, as well as communicate the importance of countering FIE threats. This will, in turn, enable the organization to leverage the appropriate capabilities to protect itself.

Best Practice #2

Identify and Assess Risks to Sensitive Assets



Purpose and Description:
Creating an inventory of sensitive information, assets, and activities enables a department or agency to focus attention on its highest priorities and ensure all are assessed for potential vulnerabilities and FIE interest. Engaging a cross-functional team with senior-level support to perform a risk assessment of these assets will ensure that all organizational missions and interests are addressed. The risk assessment, performed periodically, is the cornerstone for all security and counter-threat activities that follow.

Recommendation: The senior official, in consultation with the agency's appropriate personnel, should identify and document the agency's sensitive information, assets, and activities. Note that the collection, maintenance, and use of any personally identifiable information (PII) for this purpose should be governed by the provisions of the Privacy Act of 1974.

Recommendation: The senior official should then oversee a risk assessment process that includes these key steps:

- ☐ **Action:** Evaluate FIE threats to the agency's sensitive information, assets, and activities, including the agency's acquisitions.
- ☐ **Action:** Identify organizational vulnerabilities to threats from FIEs or malicious insiders, including physical vulnerabilities.
- ☐ **Action:** Assess the likelihood that the threat will compromise the agency's sensitive information, assets, and activities.
- ☐ **Action:** Determine adverse impact if assets are lost or compromised.
- ☐ **Action:** Identify appropriate mitigation measures.
- ☐ **Action:** Catalog threat data and additional analysis to further inform risk assessment efforts.
- ☐ **Action:** Integrate risk assessment processes and mitigation measures into the organization's program planning and budgeting cycle.
- ☐ **Action:** Establish mechanisms for continually updating the inventory of sensitive information, assets, and activities, and incorporating it into the organization's risk assessment process.

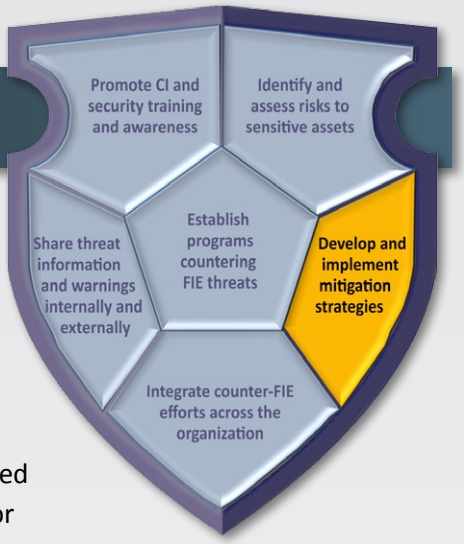
Note: Details on how to plan, organize, and execute a CI and Security Risk Assessment can be found in NCSC's *Counterintelligence/Security Risk Assessment Framework for Federal Partners*.

Sensitive information, assets, and activities include the following:

- Information classified pursuant to Executive Order 13526, Executive Order 12829, Executive Order 13549, and Executive Order 12333
- Critical infrastructure, as defined in Executive Order 13636
- Unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and U.S. government-wide policies (such information will fall under the program established under Executive Order 13556)
- National security systems, as defined by the Committee on National Security Systems (CNSS) in CNSSD-505 and CNSSI-4009 (while most systems falling under this definition are classified, not all are, and these must be designated and managed appropriately)
- Activities authorized by law or policy, as determined by departments and agencies, that would have a debilitating impact on the mission of the department or agency or on the economic or national security of the United States if compromised
- PII pertaining to individuals that is maintained within an agency's systems of records, pursuant to the Privacy Act and Executive Order 12333

Best Practice #3

Develop and Implement Mitigation Strategies



Purpose and Description:
Protective measures and mitigation strategies include an organization's decisions or actions that safeguard its sensitive information, assets, and activities from FIE threats. The measures and strategies should be commensurate with the threats to the organization and include such elements as information security measures, personnel security practices, foreign contact and visitor vetting, supply chain risk management, and prevention of unauthorized disclosures. Some of the necessary measures may require specialized training for security personnel or outreach to federal partners. In addition, this *Guide* references several documents featuring specific examples or guidelines that can support development of protective measures for the organization.

All actions should be coordinated with the appropriate responsible internal office (i.e., security, CIO, IA, IT).

Recommendation: The organization should implement protective measures and mitigation strategies to reduce its vulnerabilities to FIE threats.

Mitigating Foreign Exposure

☐ **Action:** Establish a policy requiring personnel to report—in advance—non-official foreign travel to their security office.

☐ **Action:** Brief employees traveling to high- and medium-threat locations, as appropriate, in advance of the trip, and debrief them upon return.

- For a sample reporting and debriefing guide, see the referenced *Foreign Travel Reporting Form*.

☐ **Action:** Establish policies requiring notification to security offices of all close and continuing or suspicious contact with foreign nationals by personnel with access to sensitive information, assets, and activities. Develop processes for managing notifications and response actions.

- For a sample foreign contact form, see the referenced *Foreign Contact Form*.

☐ **Action:** Establish and maintain a foreign contact repository.

☐ **Action:** Vet foreign contacts through appropriate channels to identify any affiliation with a foreign intelligence service.

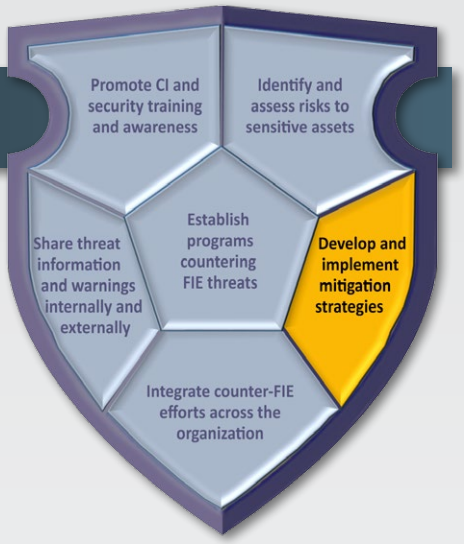
☐ **Action:** Ensure all requests by foreign nationals to visit the organization are appropriately documented. Establish and maintain an electronic record of all visits.

Note: Where possible, collection of foreign travel, foreign contact, and foreign visitor notifications should be automated and retained in a common database or information system to enable trend analysis and threat identification.

Best Practice #3

Develop and Implement Mitigation Strategies

(Continued)



Recommendation: The organization should implement protective measures and mitigation strategies to reduce its vulnerabilities to FIE threats.

Protecting Information Systems

☐ **Action:** Implement intrusion detection systems to counter unauthorized attempts to access or obtain sensitive information on your organization's networks.

☐ **Action:** Implement user activity monitoring capabilities, where able, in accordance with the *2014 Guide to Accompany the National Insider Threat Policy and Minimum Standards*.

Note: To create an effective, layered defense for information systems, organizations should ensure compliance with the *Federal Information Security Modernization Act of 2014 (FISMA)* and all National Institute of Standards and Technology (NIST) and CNSS standards.

Leveraging Reporting to Mitigate Personnel Vulnerabilities

☐ **Action:** Establish policies requiring employees to notify security personnel of suspicious incidents involving sensitive information, assets, or activities.

- See the referenced *Incident Response Form*.

☐ **Action:** Evaluate personnel security information reported by employees regarding CI concerns about themselves or others.

- Consult the Security Executive Agent National Assessment Program (SNAP) Survey for more details about designing a complete personnel security program.
- Consult the *Security Executive Agent Directive (SEAD) 3: Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position* for details about reporting requirements for relevant agency personnel.

Mitigating Supply Chain Vulnerabilities

☐ **Action:** Implement measures to mitigate vulnerabilities introduced through the organization's supply chain processes, including potential FIE access to products and services prior to acquisition, as well as vulnerabilities that emerge over the lifecycle of a product or service.

Mitigating Facilities Vulnerabilities

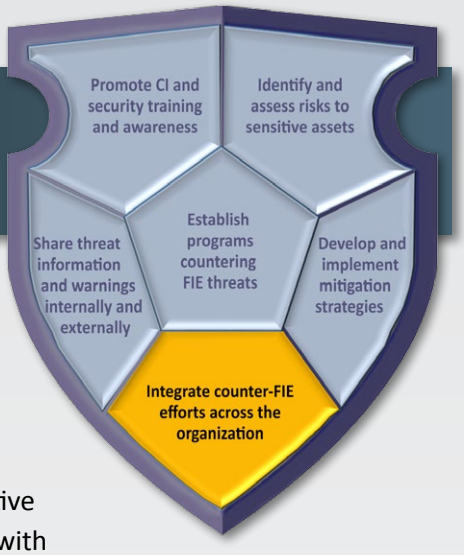
☐ **Action:** Where appropriate, implement technical surveillance countermeasures (TSCM) to safeguard sensitive information, assets, and activities.

- Consult NCSC/Technical and Cyber Directorate (TCD) for further assistance in implementing the National TSCM Program.

☐ **Action:** All classified national intelligence sensitive compartmented information (SCI) must be processed, stored, used, or discussed in accordance with *ICD 705: Sensitive Compartmented Information Facilities*.

Best Practice #4

Integrate Counter-FIE Efforts Across the Organization



Purpose and Description:
Integrating efforts to counter FIE threats into security, CI, IA, cyber, continuity of operations and continuity of government (COOP/COG), research and development, supply chain risk management, and other key functions will reduce vulnerabilities within the organization by fostering awareness and emphasizing the need to leverage all appropriate capabilities to safeguard sensitive information and assets. For example, integration of FIE threat detection efforts with acquisition functions helps prevent supply chain compromise. Safeguards against insider threats are also enhanced by engaging the widest possible range of management disciplines within an organization, including, but not limited to, HR, security, CI, IA, privacy and civil liberties, and legal.

Recommendation: The agency should develop policies, procedures and guidelines for its components that ensure the entire organization is empowered to counter FIE threats.

☐ **Action:** Develop reporting guidelines for IA, acquisition, HR, and other relevant components to share FIE threat information directly with security, CI, or other appropriate entities within the organization.

Note: The nature and extent of these policies, procedures, or guidelines shall be commensurate with the risk of FIEs targeting sensitive information within the organization and in accordance with the organization's risk management practices. The policies should serve to provide guidance to security and HR officials when CI concerns are raised during the hiring process or as part of a decision regarding access to sensitive information.

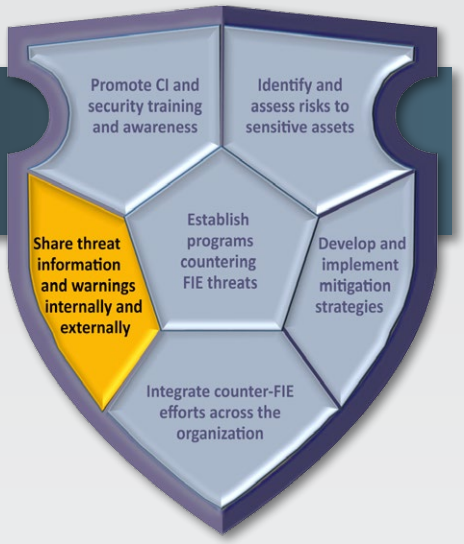
☐ **Action:** Provide security and HR officials, as well as personnel collecting or aggregating threat information, regular training regarding the collection and handling of personnel security information and the privacy, civil rights, and civil liberties of the organization's personnel and general public.

☐ **Action:** Ensure the organization's CI and appropriate security offices (network, physical, personnel) are promptly informed of all attempts to penetrate or compromise organizational resources to facilitate detection and mitigation of FIE threats.

- Where possible, your organization should establish an electronic reporting mechanism for this purpose.

Best Practice #5

Share Threat Information and Warnings Internally and Externally



Purpose and Description:
Sharing information internally is key to integrating efforts to counter FIE threats across organizational functions. Engagement and effective information sharing with external partners can ensure that threat and vulnerability reporting, partner capabilities, and best practices are leveraged to support collective safeguarding efforts.

Recommendation: The organization should share information regarding vulnerabilities and FIE threats among all relevant internal components and functions.

☐ **Action:** Establish mechanisms for sharing threat and vulnerability information among the following organizational functions:

- Counterintelligence
- Security
- Acquisitions
- Network Security/Information Assurance/Chief Information Officer
- Human Resources
- Any other relevant organizational functions

☐ **Action:** Establish mechanisms to inform network security officials of any malicious insider activity, system vulnerabilities, and FIE threats to the agency's information in order to inform cyber risk assessments and the development and implementation of appropriate technical security standards.

Note: Compromises of the organization's information systems should be reviewed by its response and recovery personnel to identify stolen or compromised content, and, with the other internal functions listed above, assess the damage caused by its loss or degradation.

Recommendation: The organization should partner with intelligence and law enforcement agencies, as necessary, to strengthen both awareness of FIE threats and the ability to respond to them.

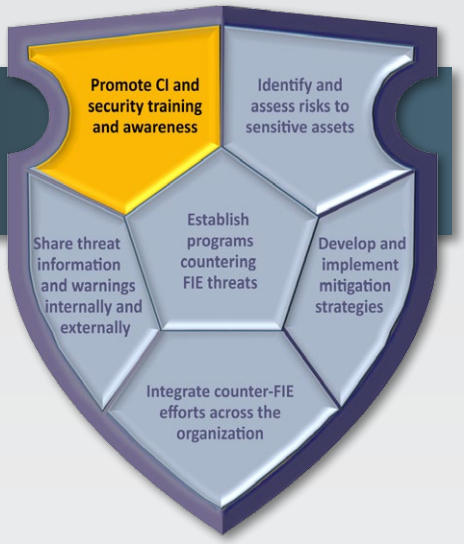
☐ **Action:** Establish mechanisms for the exchange of threat and vulnerability information between the organization and its federal external partners, to include:

- Intelligence reporting
- Common vulnerability information
- Investigative referrals
- Vetting information

☐ **Action:** Establish mechanisms for security and CI personnel to refer any suspected instances of espionage to the Federal Bureau of Investigation and other relevant federal partners.

Best Practice #6

Promote CI and Security Training and Awareness



Purpose and Description:
Threat awareness and training programs can promote a current and common understanding of FIE threats to the organization. Additionally, instructing personnel on reporting responsibilities and procedures ensures that potential threat and vulnerability information is shared in a responsible manner, so the organization can implement mitigation measures when needed.

Recommendation: The agency should continually promote workforce awareness of the threat from FIEs and provide awareness and reporting instructions to its personnel.

☐ **Action:** Develop awareness programs to address current and potential FIE threats in the work and personal environments, including:

- Information about FIEs and FIE-related cyber threats to sensitive information, assets, and activities within the organization
- FIE operational methodologies
- Organizational rules regarding the use, sharing, disclosure, storage, protection, and destruction/ disposal of sensitive information and assets, as well as the safeguarding of sensitive activities and protection of privacy, civil rights, and civil liberties
- Personnel security reporting requirements applicable to the employee's department or agency
- The risks of using online social networks and exposure of information shared on these platforms

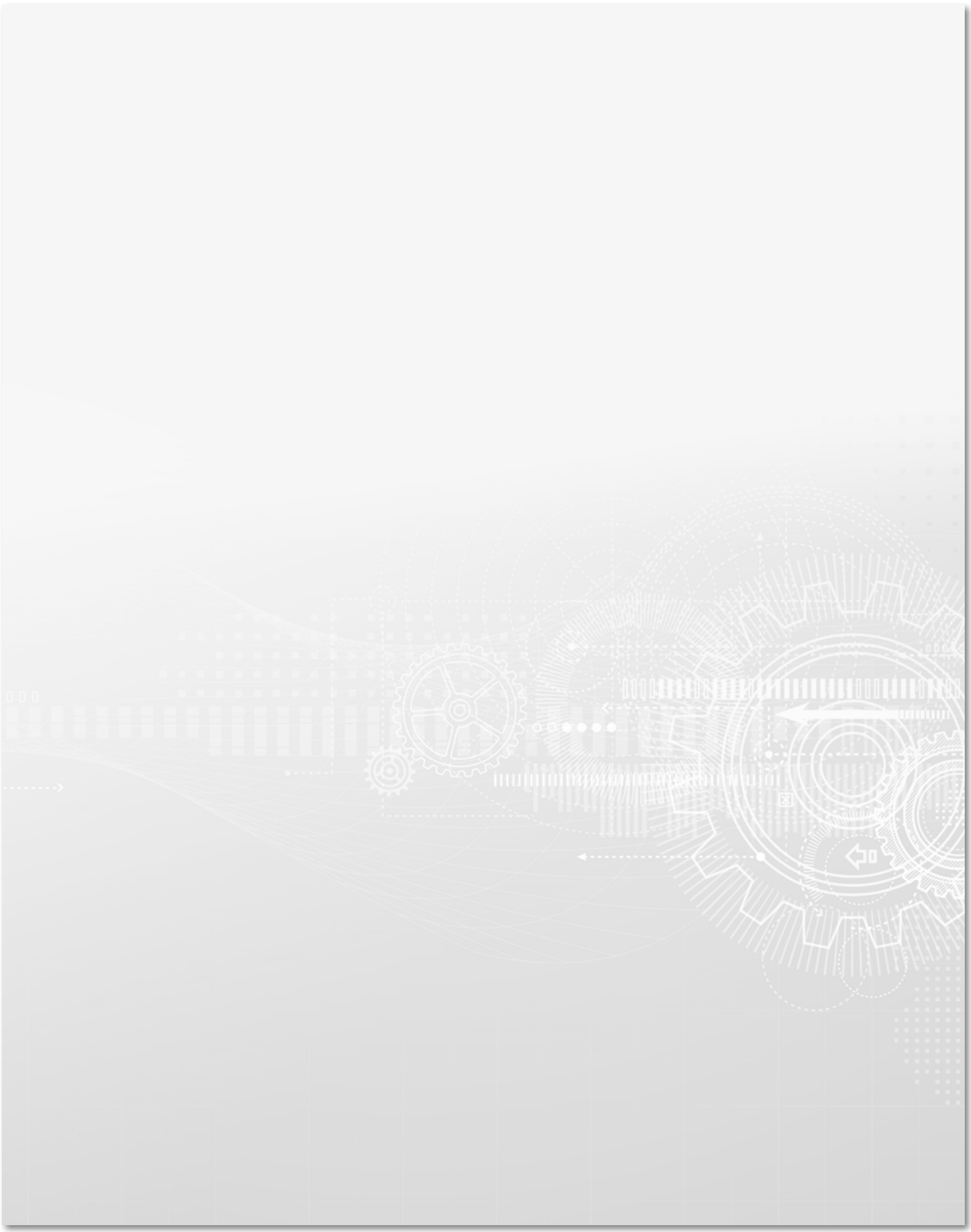
Note: Organizations should disseminate the referenced documents *Tips for Cyber Safety* and *Marking Classified National Security Information Booklet* to help inform employees of their responsibilities to protect sensitive and classified information, as well as how to protect themselves while using the Internet.

☐ **Action:** For overseas travelers, provide information about the potential for increased exposure to adversarial targeting, as well as vulnerabilities of personal and official electronic and mobile devices that may be of interest to FIEs.

☐ **Action:** For security personnel, provide technical surveillance awareness training, establish mechanisms for reporting suspected technical surveillance incidents, and engage with IC partners to receive TSCM program support and consultation on specific threats.

☐ **Action:** Develop continual awareness and reporting training for all personnel with access to sensitive information, assets, and activities.

☐ **Action:** For acquisition personnel, promote constant training and awareness of their contributing role in supply chain risk management.



Reference

Tools

2012 National Strategy for Information Sharing and Safeguarding
Reference document that provides guidance for effective development, integration, and implementation of policies, processes, standards, and technologies to promote secure and responsible information sharing.

CI and Security Risk Assessment Framework for Federal Partners
Reference document that outlines steps for establishing an assessment team, identifying sensitive assets, and conducting a CI and security risk assessment.

Foreign Travel Reporting Form
Sample form for eliciting risk-relevant information from personnel before or after foreign travel.

Foreign Contact Form
Sample form for eliciting risk-relevant information from personnel who have had substantive or close and continuing contact with a foreign national.

FY15 Annual FISMA Metrics
Description of all performance metrics developed for federal departments and agencies in support of the Federal Information Security Management Act of 2002 (FISMA).

ICCEP Self-Assessment
Self-assessment tool to aid agencies in reviewing their continuity programs and evaluating their ability to perform essential functions in case of disruptions to normal operations.

Incident Response Form
Reporting tool for providing information to security personnel on suspicious incidents involving sensitive information, assets, or activities.

ISE Data Aggregation Reference Architecture
Reference document that can enable rapid information sharing by providing a framework for interoperability between systems, applications, and organizations.

2014 Guide to Accompany the National Insider Threat Policy and Minimum Standards
Guide that provides instructions, ideas, and possible options to assist an organization in establishing a tailored program that meets the requirements of the *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*.

Protecting Key Assets Guide
Guide to conducting a risk assessment and implementing a corporate counterintelligence program to protect sensitive assets from threats from FIEs and non-state and criminal actors.

Security Executive Agent National Assessment Program (SNAP) Survey
U.S. Government Security Executive Agent survey for reviewing organizational performance in the timeliness and quality of personnel security processes.

Tips for Cyber Safety
Basic cyber awareness guide with tips for avoiding cyber threats, protecting personal data, and using the Internet safely and responsibly.

Marking Classified National Security Information Booklet
Guide for properly marking classified information.

Reference (continued)

Guiding Documents

National Counterintelligence Strategy of the United States of America 2016

National Insider Threat Policy and Minimum Standards, 21 Nov 2012

Executive Order 12333 - United States Intelligence Activities

Executive Order 12829 – National Industrial Security Program

Executive Order 12968 – Access to Classified Information

Executive Order 13526 – Classified National Security Information

Executive Order 13549 – Classified National Security Information Programs for State, Local, Tribal and Private Sector Entities

Executive Order 13556 – Controlled Unclassified Information

Executive Order 13587 – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information

Executive Order 13636 – Improving Critical Infrastructure Cybersecurity

Federal Information Security Management Act of 2002 (FISMA)

Federal Information Security Modernization Act of 2014 (FISMA)

Presidential Decision Directive/NSC-12 (PDD-12): Security Awareness and Reporting of Foreign Contacts

SEAD-1: Security Executive Agent Authorities and Responsibilities

SEAD-3: Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position

SEAD-5: Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications

Counterintelligence Enhancement Act of 2002

Privacy Act of 1974

Useful Resources

ICD 700 – Protection of National Intelligence

ICD 702 – Technical Surveillance Countermeasures

ICD 703 – Protection of Classified National Intelligence, Including Sensitive Compartmented Information

ICD 705 – Sensitive Compartmented Information Facilities

ICD 731 – Supply Chain Risk Management

ICD 750 – Counterintelligence Programs

CNSSD No. 505 – Committee on National Security Systems Directive, Supply Chain Risk Management

CNSSI No. 4009 – Committee on National Security Systems Instruction, National Information Assurance (IA) Glossary

NIST 800-53 (rev.4) – Security and Privacy Controls for Federal Information Systems and Organizations

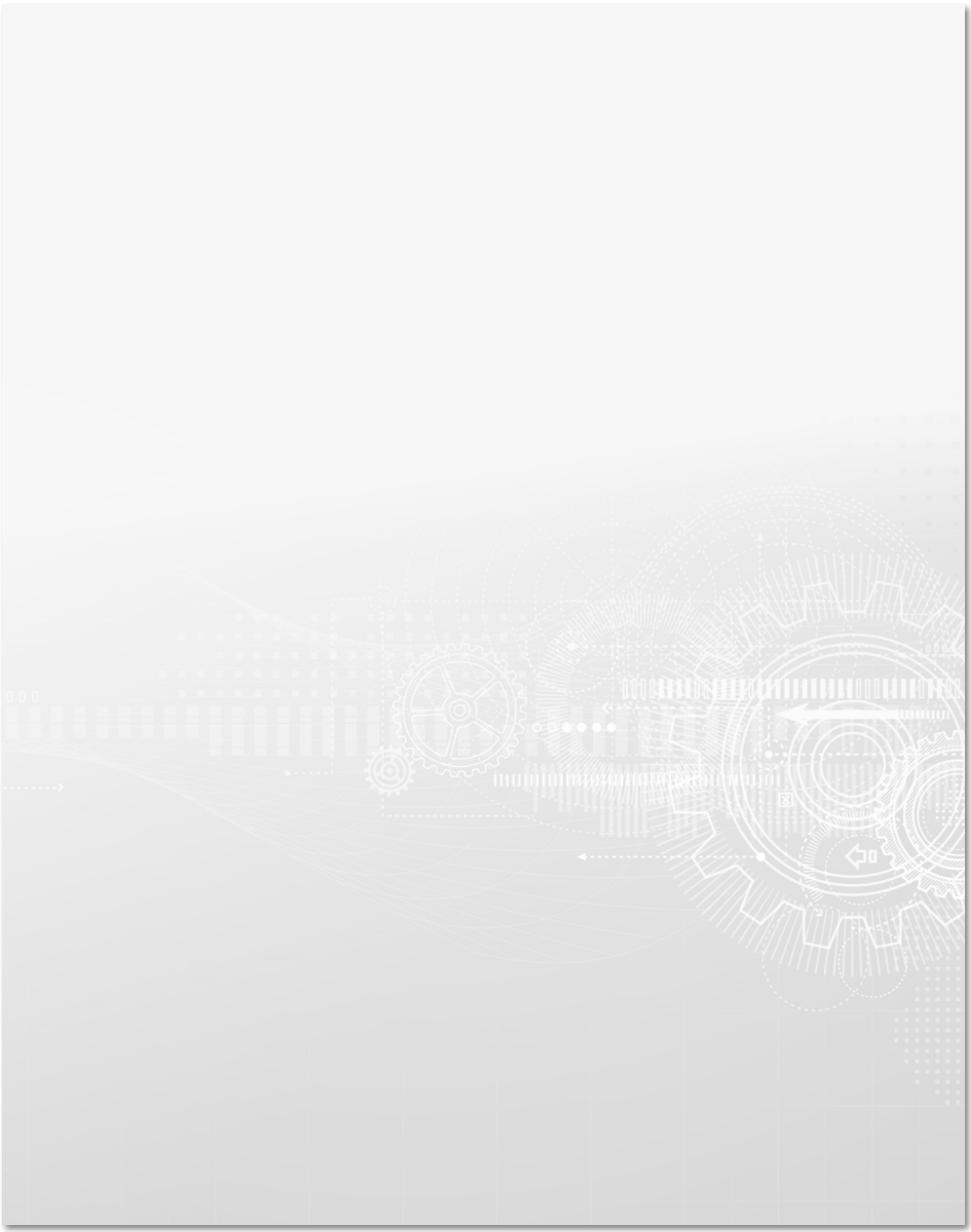
NIST 800-53A (rev.4) – Assessing Security and Privacy Controls in Federal Information Systems and Organizations

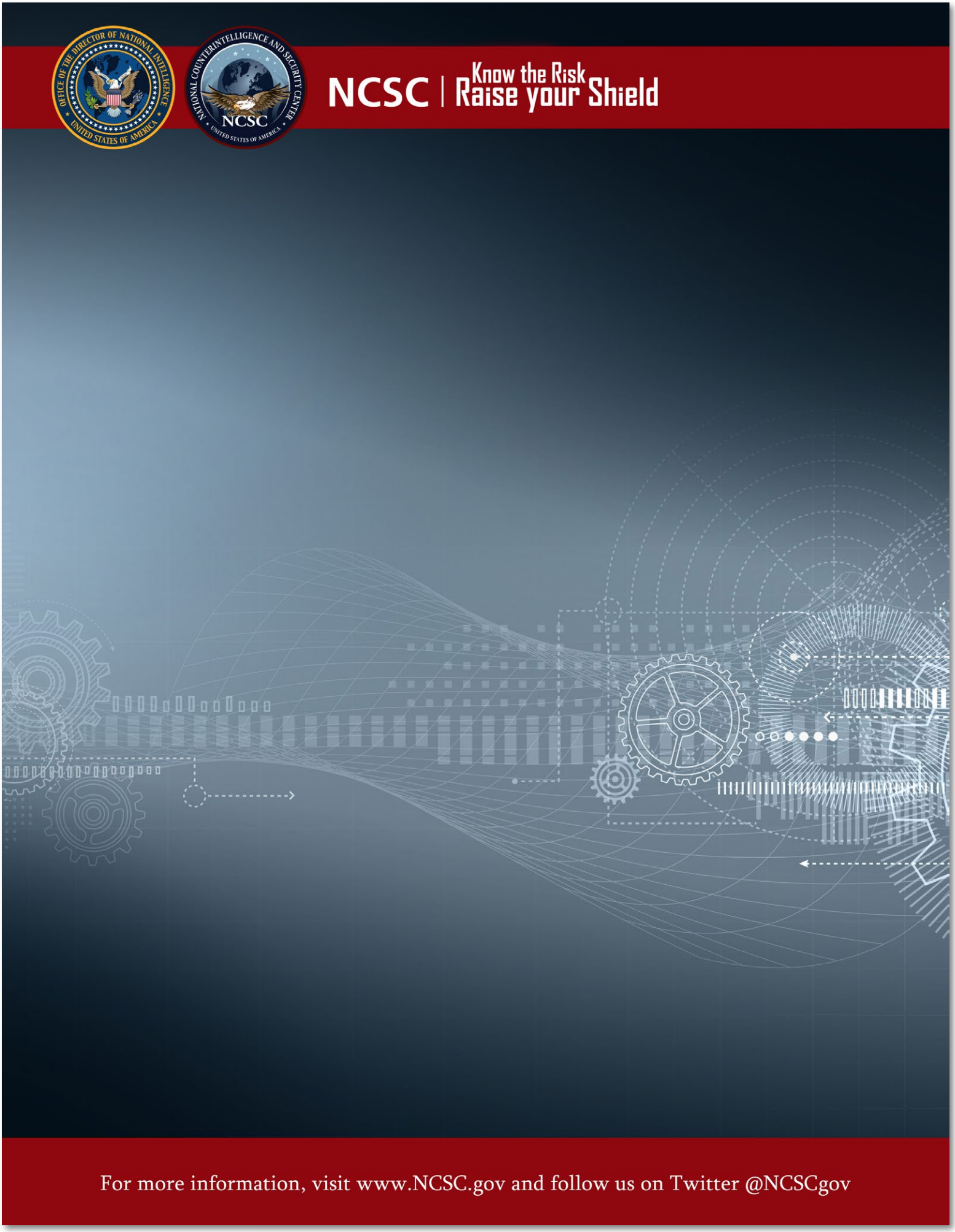
Reference (continued)

Active Partnership

For access to the following and to engage NCSC's staff in ongoing support, visit NCSC.gov:

- Awareness materials
- Protecting Personal Information campaign materials
- Training modules and courses
- Threat briefings
- Assessment findings and reports




NCSC | Know the Risk Raise your Shield
For more information, visit www.NCSC.gov and follow us on Twitter @NCSCgov