

Enterprise Risk Mitigation Blueprint for Non-Intelligence Agencies



NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER



2023



Contents

Protect Your Organization	1
Preamble	1
Introduction	1
Threat Overview	2
Enterprise Risk Mitigation – Blueprint	3
Enterprise Risk Mitigation – Self Evaluation	3
Enterprise Risk Management – Best Practices	5
Put It All Together	9
References, Resources, and Terms	10
Notes	11



Protect Your Organization from the Foreign Intelligence Threat

Enterprise Risk Mitigation Blueprint

Preamble

Nothing in this document shall be construed as authorization for any organization to conduct activities not otherwise authorized under statutes, 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.

Threats are not limited to only cyber, insider, foreign intelligence and/or criminal activities.

Introduction

Today's global threat environment is more diverse and dynamic than ever. The 2023 Annual Threat Assessment of the U.S. Intelligence Community (IC) ¹ identified a growing number of foreign intelligence entities (FIE), state actors, and non-state actors targeting the United States Government (USG) and the private sector. They are no longer interested just in obtaining classified U.S. secrets, but are also collecting sensitive unclassified information from most government agencies and virtually every sector of our economy. Personal data, trade secrets, intellectual property, technology, and research and development are being aggressively targeted by adversaries who have the capability, patience, and resources to obtain them.

To achieve their objectives, FIEs are employing a wide range of illegal techniques including insider threats, cyber penetrations, supply chain attacks, and blended operations that combine some or all of these methods. They are also using a variety of legal and quasi-legal methods, including mergers and acquisitions, investment, joint ventures, partnerships, and talent recruitment programs to acquire U.S. technology and innovation. Ultimately, FIEs seek to degrade our economic power and national security, compromise our critical infrastructure, and undermine our democratic institutions.

This new form of conflict is not fought on a foreign battlefield but in our power grids, our computer networks, our laboratories and research facilities, our financial institutions, our healthcare systems, and our federal, state, local, and tribal governments. This challenge can be met only by hard work, determination and diligence, and public and private sector partnership.

Ultimately, FIEs seek to degrade our economic power and national security, compromise our critical infrastructure, and undermine our democratic institutions.

NCSC is working closely with partners to implement holistic, integrated enterprise risk mitigation (ERM) programs to develop a "blended" enterprise approach, actively engaging the entire enterprise to protect their organizations. Our citizens as well as our government

¹ <https://www.intelligence.senate.gov/resources>



and institutions need capabilities that deter our adversaries capabilities. These capabilities can be provided by an integrated and layered ERM program. This document includes links to risk mitigation information that can help organizations enhance their physical security, personnel security, operations security (OPSEC), cybersecurity, defensive counterintelligence (CI), insider threat mitigation capabilities, and supply chain risk management (SCRM).

ERM programs mitigate vulnerabilities to protect critical assets from collection, theft, disruption, and exploitation. A well-developed program likely will have the added benefit of protecting the organization against criminal exploitation as well. Successful threat mitigation requires leveraging the workforce at all levels across an organization.

Threat Overview

Some foreign governments combine civilian and military capabilities with criminal activity to steal information to gain an advantage. These practices illustrate the blurred lines between traditional intelligence collection and economic espionage.

Rapid technological advancements are enabling FIEs to refine cyber capabilities and target organizations in the United States. Their cyber operations penetrate our government and private sector in pursuit of policy insights, research, intellectual property, military and trade secrets, and personal identifiable information (PII), all to obtain a competitive advantage.

There are also significant risks associated with our nation's ever-increasing reliance on interconnected information technologies, particularly across critical infrastructure sectors such as the defense industrial base, energy, finance, healthcare, and telecommunications.

Additionally, many state actors view economic espionage—often using commercial enterprises owned or influenced by the state—as essential to achieving their own national security and economic goals. This comes at our expense.

FIEs attempt to exploit vulnerabilities in government and industry supply chains to steal our intellectual property, corrupt our software, surveil our critical infrastructure, and carry out other malicious activities through cyber or technical operations. FIE tactics have included elicitation, economic espionage, human targeting, and cyber intrusions.

FIE tactics have included elicitation, economic espionage, human targeting, and cyber intrusions.

We are increasingly concerned about state and non-state-sponsored attempts to control or debilitate critical infrastructure systems, corrupt supply chains, or gain access to systems that control our nation's critical infrastructure. The systemic and persistent vulnerabilities continue to grow, intensifying traditional FIE threats, placing critical infrastructure and emerging and proprietary technologies at risk, eroding competitive advantage, and weakening our global influence.

The federal workforce is one of our nation's greatest assets, but it faces an increasingly challenging risk environment ranging from insider threats, unauthorized disclosures, workplace violence, and being targeted by adversaries. These workforce challenges will persist.

Threat actors are conducting malicious influence campaigns that employ cyber operations, propaganda, and manipulation to try to sow divisions in society and undermine confidence in democratic institutions.²

Enterprise Risk Mitigation – Blueprint

This ERM blueprint offers a perspective about threat mitigation to help organizations better understand shared intended outcomes and take inventory of the capabilities necessary to effectively mitigate and counter enterprise-wide threats. This framework can be applied to assist your organization's mission needs by using existing governance structures or by creating new ones. There are common principles that are shared by all successful ERM programs:

- ☐ The program's intent originates from the organization's leadership and represents their shared vision
- ☐ A clear and concise mission statement is produced
- ☐ The program's limitations are clearly defined and conform to law
- ☐ The organization's leadership embraces the vision and prioritizes the mission
- ☐ Leadership demonstrates and models program behaviors and support for the mission
- ☐ Leadership maintains unfettered two-way communication with program management
- ☐ The program is scalable and supports the entire organization, regardless of location
- ☐ The program develops appropriate standard operating procedures (SOP)
- ☐ The program has policies for referrals for jurisdiction
- ☐ The program is centrally managed and executed
- ☐ The program is regularly inspected for compliance
- ☐ Sensitive issues are reported and addressed in a timely and discreet manner

Enterprise Risk Mitigation – Self Evaluation

The first steps of an ERM program will begin with a periodic sequenced series of structured inventories, assessments, and analysis as part of a self-evaluation process. The results will be a prioritized list of critical assets and a plan to mitigate organization vulnerabilities. A sample self-evaluation process follows.

1. Identify Critical Assets
2. Vulnerability Assessment
3. Threat Assessment(s)
4. Risk Assessment
5. Vulnerability Mitigation Plan
6. Prioritized List of Critical Assets

² <https://www.dni.gov/index.php/fmic-what-we-do>

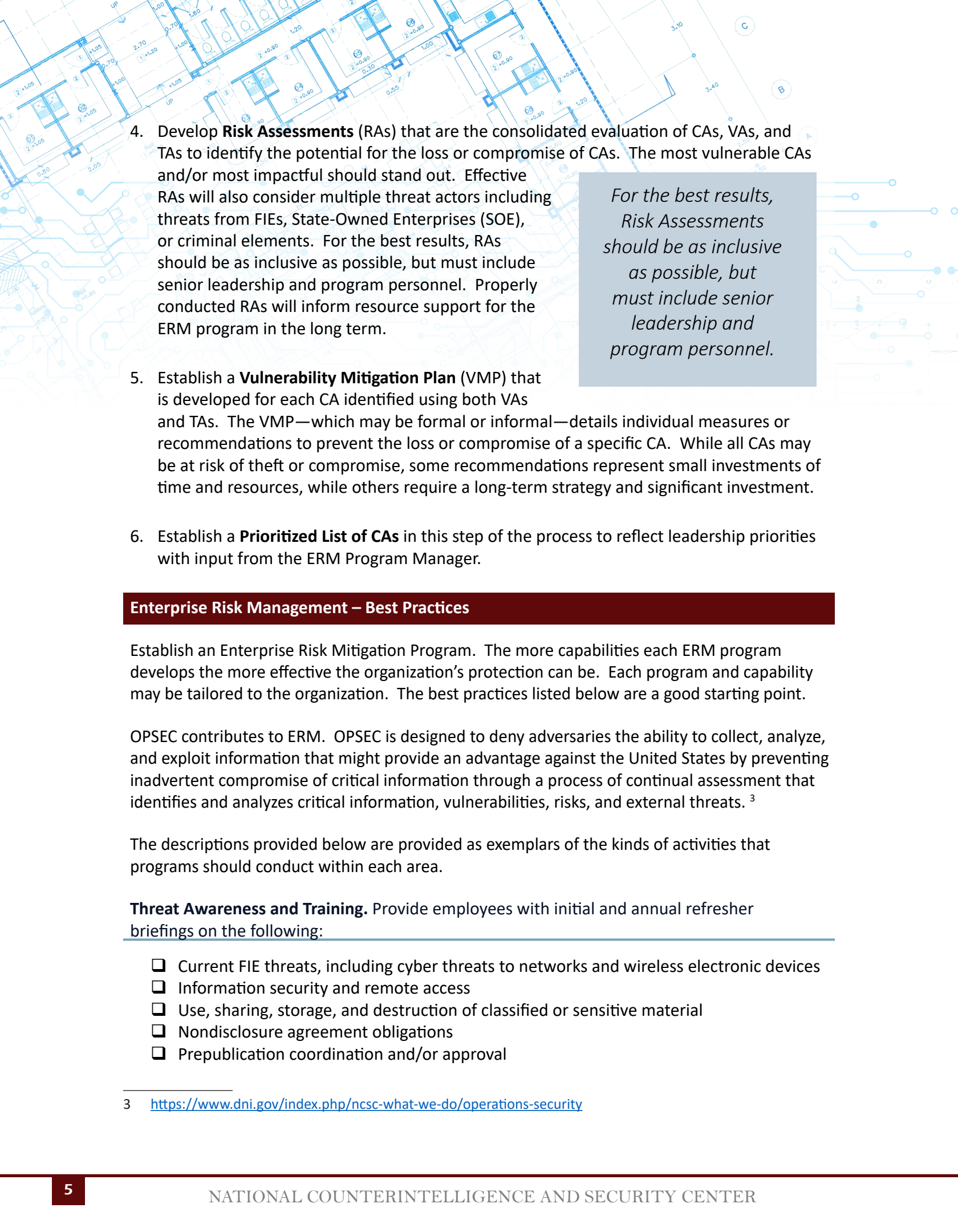
1. Identify **Critical Assets (CAs)**, and the loss or compromise of what could negatively affect the organization's mission that may include:

- ☐ Items necessary for the organization to accomplish its mission
- ☐ Intellectual property, and/or trade secrets, and information unique to the organization
- ☐ Sensitive, emerging, and proprietary technologies, research, and development
- ☐ Classified and/or sensitive but unclassified information
- ☐ Employees, key personnel, personal identifiable information, groups, and relationships
- ☐ Contracts and supply chain information
- ☐ Communications, computer networks, and facilities
- ☐ Big data, investments, financial, regulatory, and economic information
- ☐ Information impacting the organization's reputation
- ☐ Access to policymakers, information on policies, and negotiating strategies

2. Conduct **Vulnerability Assessments (VAs)**, that are comprehensive reviews of an organization's security posture, and organizational weaknesses, as determined through research, analysis, direct observation, and collection of information from the organization's employees. The organization should attempt to identify systemic, programmatic, or institutional vulnerabilities that may contribute to the potential compromise or exploitation of a CA.

3. Conduct **Threat Assessments (TAs)** that are developed by a few specialized organizations that have an intelligence function or responsibility for U.S. law enforcement. TAs may be developed in various forms, but most often they have a geographical, functional, and/or threat actor focus. Domestic TAs often have a criminal threat component. For our purposes, TAs focus primarily on the interests and capabilities of FIEs, but may also include criminal elements. TAs published from sensitive or classified sources are usually not available for public distribution. However, if there has been a determination that public release of the information is in the national interest, information may be released, through appropriate channels. The cleared ERM program manager acts as the organization's focal point for classified and unclassified TA content, and may act as an advocate for the development of unclassified talking points for public release or broad organization consumption. The following IC partners can aid in identifying and accessing existing TAs:

- ☐ Federal Bureau of Investigation (FBI)
- ☐ Department of Homeland Security
- ☐ National Counterintelligence and Security Center (NCSC)

- 
4. Develop **Risk Assessments (RAs)** that are the consolidated evaluation of CAs, VAs, and TAs to identify the potential for the loss or compromise of CAs. The most vulnerable CAs and/or most impactful should stand out. Effective RAs will also consider multiple threat actors including threats from FIEs, State-Owned Enterprises (SOE), or criminal elements. For the best results, RAs should be as inclusive as possible, but must include senior leadership and program personnel. Properly conducted RAs will inform resource support for the ERM program in the long term.
 5. Establish a **Vulnerability Mitigation Plan (VMP)** that is developed for each CA identified using both VAs and TAs. The VMP—which may be formal or informal—details individual measures or recommendations to prevent the loss or compromise of a specific CA. While all CAs may be at risk of theft or compromise, some recommendations represent small investments of time and resources, while others require a long-term strategy and significant investment.
 6. Establish a **Prioritized List of CAs** in this step of the process to reflect leadership priorities with input from the ERM Program Manager.

For the best results, Risk Assessments should be as inclusive as possible, but must include senior leadership and program personnel.

Enterprise Risk Management – Best Practices

Establish an Enterprise Risk Mitigation Program. The more capabilities each ERM program develops the more effective the organization's protection can be. Each program and capability may be tailored to the organization. The best practices listed below are a good starting point.

OPSEC contributes to ERM. OPSEC is designed to deny adversaries the ability to collect, analyze, and exploit information that might provide an advantage against the United States by preventing inadvertent compromise of critical information through a process of continual assessment that identifies and analyzes critical information, vulnerabilities, risks, and external threats.³

The descriptions provided below are provided as exemplars of the kinds of activities that programs should conduct within each area.

Threat Awareness and Training. Provide employees with initial and annual refresher briefings on the following:

- ☐ Current FIE threats, including cyber threats to networks and wireless electronic devices
- ☐ Information security and remote access
- ☐ Use, sharing, storage, and destruction of classified or sensitive material
- ☐ Nondisclosure agreement obligations
- ☐ Prepublication coordination and/or approval

³ <https://www.dni.gov/index.php/ncsc-what-we-do/operations-security>

- ☐ Foreign travel and foreign contact reporting
- ☐ Outside activity reporting
- ☐ Indicators of Insider Threat and reporting
- ☐ The Nationwide Suspicious Activity Reporting Initiative ⁴

Insider Threat: ⁵

- ☐ Use technology to get a better sense of workforce behavior, particularly within virtual domains
- ☐ Build a program that identifies individual anomalous behavior
- ☐ Establish policy to address anomalous behavior in a way that fosters trust in the organization

Visitor and Assignee Vetting:

- ☐ Establish policy for controlled access to organization facilities
- ☐ Establish policy to maintain local and/or centralized visitor logs
- ☐ Establish policy for use of the National Vetting Center ⁶

Foreign Contact Reporting, Briefing, and Debriefing:

- ☐ Establish policy for notification of contact with a foreign national
- ☐ Establish policy for a foreign contact log ⁷

Foreign Travel Reporting, Briefing, and Debriefing:

- ☐ Establish policy for advance notification of foreign travel
- ☐ Establish policy for maintaining foreign travel logs
- ☐ Establish policy to conduct pre-brief of threats to employees traveling to high-threat locations, and appropriate debriefs upon their return
- ☐ Establish policy to capture significant reporting from the debriefs to share with other government organizations

Support to Security and Information Assurance:

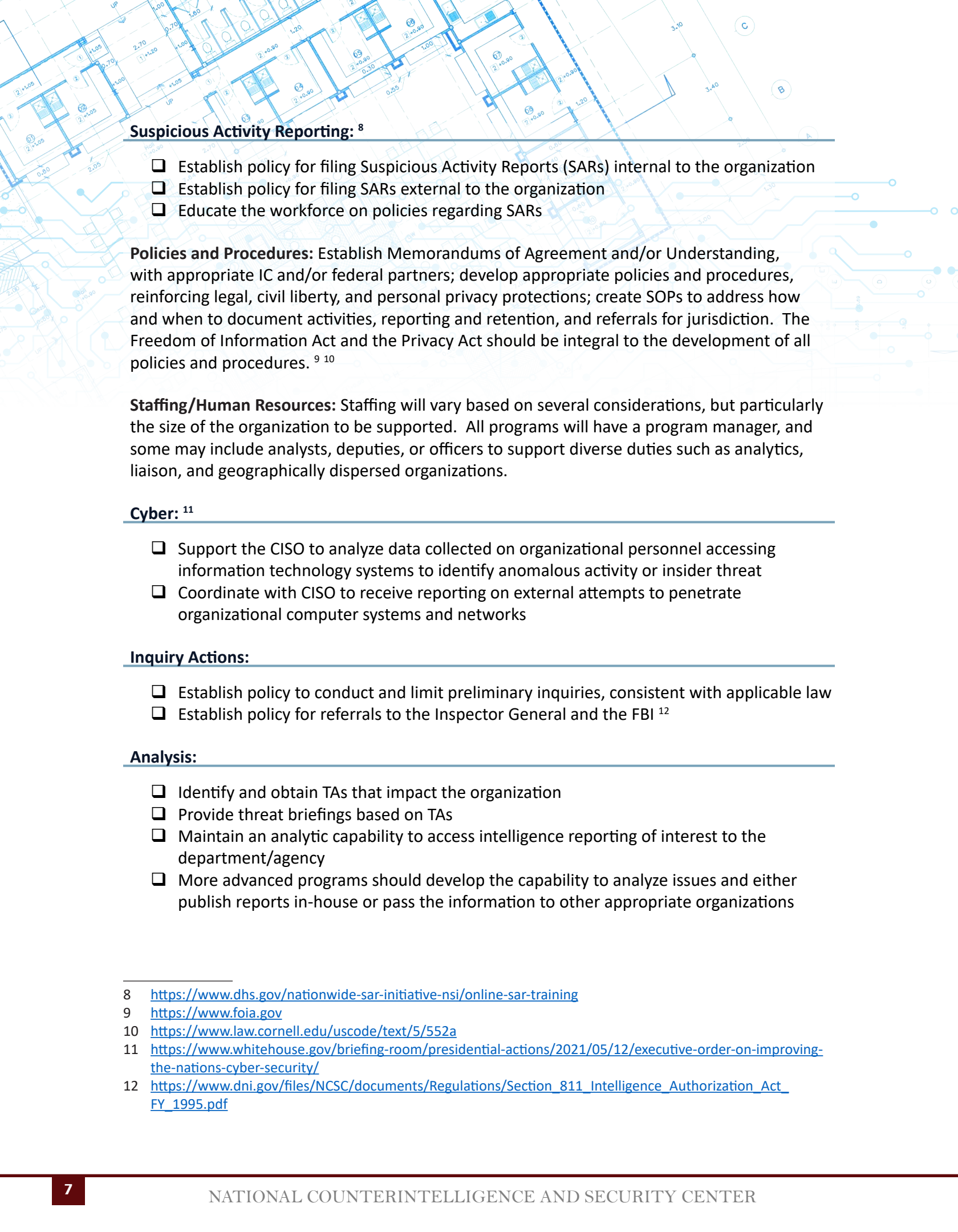
- ☐ Support to identify threats and vulnerabilities
- ☐ Support sensitive and/or compartmented programs
- ☐ Develop and execute vulnerability mitigation plans for CAs in the department
- ☐ Support security clearance activities and “need-to-know” principle
- ☐ Support rules regarding subsequent use, storage, and destruction of classified material
- ☐ Support prepublication review obligations
- ☐ Support Chief Information Security Office (CISO) activities for auditing and monitoring on government computers
- ☐ Support for the use of non-disclosure agreements and confidentiality agreements

⁴ <https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-insider-threat>

⁵ <https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-insider-threat>

⁶ <https://www.cbp.gov/border-security/ports-entry/national-vetting-center>

⁷ <https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf>



Suspicious Activity Reporting: ⁸

- ☐ Establish policy for filing Suspicious Activity Reports (SARs) internal to the organization
- ☐ Establish policy for filing SARs external to the organization
- ☐ Educate the workforce on policies regarding SARs

Policies and Procedures: Establish Memorandums of Agreement and/or Understanding, with appropriate IC and/or federal partners; develop appropriate policies and procedures, reinforcing legal, civil liberty, and personal privacy protections; create SOPs to address how and when to document activities, reporting and retention, and referrals for jurisdiction. The Freedom of Information Act and the Privacy Act should be integral to the development of all policies and procedures. ^{9 10}

Staffing/Human Resources: Staffing will vary based on several considerations, but particularly the size of the organization to be supported. All programs will have a program manager, and some may include analysts, deputies, or officers to support diverse duties such as analytics, liaison, and geographically dispersed organizations.

Cyber: ¹¹

- ☐ Support the CISO to analyze data collected on organizational personnel accessing information technology systems to identify anomalous activity or insider threat
- ☐ Coordinate with CISO to receive reporting on external attempts to penetrate organizational computer systems and networks

Inquiry Actions:

- ☐ Establish policy to conduct and limit preliminary inquiries, consistent with applicable law
- ☐ Establish policy for referrals to the Inspector General and the FBI ¹²

Analysis:

- ☐ Identify and obtain TAs that impact the organization
- ☐ Provide threat briefings based on TAs
- ☐ Maintain an analytic capability to access intelligence reporting of interest to the department/agency
- ☐ More advanced programs should develop the capability to analyze issues and either publish reports in-house or pass the information to other appropriate organizations

⁸ <https://www.dhs.gov/nationwide-sar-initiative-nsi/online-sar-training>

⁹ <https://www.foia.gov>

¹⁰ <https://www.law.cornell.edu/uscode/text/5/552a>

¹¹ <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cyber-security/>

¹² https://www.dni.gov/files/NCSC/documents/Regulations/Section_811_Intelligence_Authorization_Act_FY_1995.pdf

Supply Chain.¹³ The global nature of critical supply chains increases the threat for targeting and exploitation of our critical infrastructure. Foreign adversaries are attempting to access our nation's key supply chains at multiple levels from concept to design, manufacturing, integration, deployment, and maintenance by a variety of means. Securing critical supply chains from FIE attempts to compromise the integrity, trustworthiness, and authenticity of products and services purchased and integrated into the operations of organizations is an enduring security challenge.

Supply Chain Risk Management must be a priority throughout the acquisition-process lifecycle. Consider the following:

- ☐ Illuminate the supply chain
- ☐ Establish supply chain integrity
- ☐ Identify and manage supply chain vulnerabilities
- ☐ Secure supply chain from FIE exploitation
- ☐ Develop mitigation strategies for vulnerabilities presented by the supplier, the supply chain, or the product and its subcomponents
- ☐ Validate commercial off-the-shelf software origins and manufacturers

Critical Infrastructure: There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on national and/or economic security, or public health and safety. Efforts should be made to support national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure.¹⁴

Much of our nation's critical infrastructure is owned and operated by industry. Key sectors, including transportation, banking, water, and healthcare are at risk unless stakeholders understand the threat and adopt appropriate security standards.

Key sectors, including transportation, banking, water, and healthcare are at risk unless stakeholders understand the threat and adopt appropriate security standards.

Technologies and Intellectual Property Vulnerabilities: Scientific discovery and innovation empower the United States with a competitive edge that enhances our military capability and propels our economy. Our culture of openness and collaboration in science and technology makes our national labs, universities, and industry high-value targets for economic espionage. The foreign threat to intellectual property is growing as measured by FBI investigations, criminal convictions, and the number and sophistication of cyber intrusions.^{15 16}

13 <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/>

14 <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>

15 <https://www.dni.gov/index.php/safeguarding-science>

16 <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/>

Put It All Together

To mitigate risk, the best practices and protocols identified herein must be fully integrated into organizational culture, operational programs, corporate policies, practices, and procedures. Countering foreign intelligence threats requires an integrated approach across the organization to ensure both human and technical intelligence threats are addressed in a coordinated, holistic manner and that all security disciplines operate together seamlessly.

One of NCSC's core missions is to support and partner with organizations by providing subject matter experts, reference materials, and advocacy activities to help create an integrated approach to countering foreign adversarial threats. For additional information on NCSC awareness or materials, visit NCSC at [NCSC.gov](https://www.ncsc.gov) or contact us at NCSC_Outreach@odni.gov



References, Resources, and Terms

1. Counterintelligence Glossary, Center for Development of Security Excellence
<https://www.cdse.edu/Portals/124/Documents/glossary/CI-glossary.pdf>
2. The Counterintelligence Enhancement Act of 2002, as amended and Executive Order 12333, as amended, 2008 and Intelligence Reform and Terrorism Prevention Act, 2004
<https://www.dni.gov/files/documents/OGC/IC-Legal-Reference-Book-2020.pdf>
3. National Counterintelligence Strategy of the United States of America
<https://www.dni.gov/index.php/ncsc-home>
4. Terms and Definitions of Interest for Counterintelligence Professionals, 2 May 2011
https://www.dni.gov/files/NCSC/documents/ci/CI_Glossary.pdf
5. The Center for the Development of Security Excellence
<https://www.cdse.edu>
6. The Committee for Foreign Investment in the United States (CFIUS) of the Department of the Treasury
<https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius>
7. The Bureau of Industry and Security of the Department of Commerce
<https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list>

Notes





OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE