THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

ENTERPRISE THREAT MITIGATION

THIS PRODUCT WAS PRODUCED BY NCSC'S ENTERPRISE THREAT-MITIGATION DIRECTORATE AND THE NATIONAL INSIDER THREAT TASK FORCE

A CAPABILITES-DRIVEN FRAMEWORK FOR THREAT MITIGATION

A new way of understanding how to mitigate the growing scope and magnitude of the adversarial threat to our nation.

Each organization of the U.S. Government is extremely diverse and no two have the same hierarchy or organizational structure. Counterintelligence, traditional security disciplines, cybersecurity, human resources, insider threat, acquisitions, and other core business programs often have their own set of policies, fall under different chains of command, and are sometimes separated at the senior-most level of organizations.

In contrast, sophisticated threats – also known as advanced persistent threat (APT)[1] – such as those from nation states, foreign intelligence services, or advanced criminal enterprises – use well-coordinated, blended, offensive practices to gain access to your high-valued assets.[2] At its core, APT is a human threat, with threat actors or their agents seeking to achieve their objectives. APT is human intelligence. It is orchestrated and unwavering.

The end-goal is to make our high-valued assets harder targets by understanding, anticipating, and mitigating threats.

Our federal institutions, information, facilities, and personnel need a defensive capability that *exceeds* the adversarial blended offensive capability. The federal security posture should be about enterprise defense, encompassing each department and organization – headquarters and field elements. Enterprise defense needs to be distributed across organizations and across security domains where all disciplines are operating in mutual support of one another to establish a true unity of effort. More effective and distributed enterprise defense is going to require both improved knowledge of the threat and of our own security postures.

To this end, the National Counterintelligence and Security Center (NCSC) and the Enterprise Threat-Mitigation Directorate (ETD) offers this capabilities-driven framework for integrating defensive capabilities – most of which already reside within your organizations – to create a blended, distributed defense capability. The concepts highlighted in this framework are not new and exist in numerous federal laws, regulations,

[1] The National Institute of Standards and Technology (NIST) Publication SP 800-39, *"Managing Information Security Risk: Mission and Information System View,"* https://csrc.nist.gov/publications/detail/sp/800-39/final

[2] High Value Asset definition: Those information resources, mission/business processes, and/or critical programs that are of particular interest to potential or actual adversaries. https://www.dnss.gov/CNSS/openDoc.cfm?nlpeHdTd15WNb/cCDa97qA==)

policies, and guides that have been published and widely distributed. One such guide that stands the test of time is the, Countering Foreign Intelligence Threats: Implementation and Best Practices Guide (CFIT).[3] This guide was issued by NCSC in 2017 and was written specifically with foreign intelligence threats in mind. The concepts are certainly still valid today and are reflected in this framework as applicable to countering ALL adversarial threats across a broad spectrum.

What *has* changed is the scope and magnitude of the adversarial threat to our nation – threats from a greater number of adversaries, with increasingly sophisticated capabilities, targeting a much broader set of targets.[4] Ensuring U.S. interests are protected in the midst of this threat requires a risk-based, comprehensive, whole-of-nation effort. We need a fundamental, cultural shift in how we think about mitigating this threat.

This framework offers a new way of thinking about threat mitigation and a way of gathering and using the critical elements – that already exist – to help organizations better understand our shared **intended outcomes** and those **capabilities** necessary to effectively mitigate and counter enterprise-wide threats. We understand organizations already have a number of security requirements and limited resources. This framework can be modified to meet your organization's unique mission needs – using or restructuring existing governance structures that encompass these elements, or by creating new ones.

Shared Intended Outcomes for Effective Enterprise Threat Mitigation:

The end-goal is to make our high-valued assets harder targets by understanding, anticipating, and mitigating threats[5] – regardless of the organization's mission, size, structure, or culture.

- **Your organization's entire workforce – from the entry-level employee to the head of the organization –understands the adversarial threat and risks[6] to the organization.**
  Only by understanding the threat and risks can our employees serve as the first line of defense.
  - Be aware of the adversarial threat (intent and capability) and incorporate it into the organization's risk management calculus.[7]

- **Your organization is engaged with its workforce to create and continuously promote a culture of security and inclusion.**
  - Your organization's workforce is the most highly valued asset and should be a trusted

[3] *"Countering Foreign Intelligence Threats: Implementation and Best Practices Guide,"* Published by the National Counterintelligence and Security Center (NCSC) in 2017, https://www.dni.gov/files/NCSC/documents/campaign/Guid_CFIT-Implementation-and-Best-Practices-Guide_2017-06-08_UNCLASS_LINKED.pdf

[4] 2020-2022 National Counterintelligence Strategy of the United States, https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf

[5] Threat definition: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. .(NIST Glossary: https://www.dnss.gov/CNSS/openDoc.cfm?nlpeHdTd15WNb/cCDa97qA==)

[6] Risk definition: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. .(NIST Glossary: https://www.dnss.gov/CNSS/openDoc.cfm?nlpeHdTd15WNb/cCDa97qA==)

[7] National Security Presidential Memorandum (NSPM) 28, "*The National Operations Security (OPSEC) Program,"* January 13, 2021, JWICS site: https://www.ncsc.ic.gov/etd/docs/NCSC-21-00137_Memo_National_Operations_Security_Program.pdf.pdf

partner in the enterprise-wide mitigation of threat.
  - Alongside the need to understand the threat and risks, your entire organization's workforce must understand they are the organization's most important resource AND the most effective player in your enterprise-wide efforts to ensure national and economic security.
  - The most effective enterprise threat-mitigation efforts include:
    - Coordinated and cross-cutting training and awareness campaigns;
    - Proactive campaigns to include the workforce in threat information/intelligence efforts; and
    - Leadership and supervisory training.

- **Adversarial threats are included in all your organizational risk-management practices.**
  You must take stock of your enterprise-wide risk posture.
  - Identify high-valued assets – organizations should consider the broad strategic value of their assets in terms of missions and operations; from a national and economic security perspective, AND from the adversary's perspective. View your resources through the eyes of the adversary – then identify all pathways to those resources and defend them.[8]
  - Identify all pathways, or threat vectors, to high-valued assets and where they cross – sophisticated threat actors are not only capable of using different threat vectors of attack (e.g., physical intrusion, cyber attacks, insider threats, etc.); they are also capable of crossing threat vectors thus creating vulnerabilities and executing blended attacks.
  - To counter our adversaries' ability to migrate across threat vectors, it is more important than ever for counterintelligence and security professionals from all disciplines have a robust understanding of each other's roles and responsibilities.
  - Consider ALL pathways – including your own people, who are the highest valued assets in any organization.

- **Your organization has an effective threat intelligence[9] capability.**
  To understand and effectively mitigate the enterprise-wide threats we face, organizations need access to external sources of threat intelligence and need to be able to generate, use, and share their own intelligence.
  - Large organizations and those facing extreme adversarial threats, may need to have a resourced and dedicated threat intelligence program.[10]
  - Those organizations with a mature threat intelligence capability have the inherent responsibility to assist those agencies that need to develop and mature their capabilities.

- **Your organization has proactive and coordinated incident response practices.**
  - Sophisticated threat actors will not stop until they get to the high-valued assets they seek.

[8] OMB Memorandum 2019-03, *"Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program,"* https://www.whitehouse.gov/wp-content/uploads/2019/03/M-19-13.pdf.
[9] Threat intelligence definition: Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.(NIST Glossary: https://www.dnss.gov/CNSS/openDoc.cfm?nlpeHdTd15WNb/cCDa97qA==)
[10] National Counterintelligence and Security Center (NCSC) *"Insider Threat Mitigation for U.S. Critical Infrastructure Entities Guide,"* This guide describes the basic functions of a threat intelligence program, https://www.dni.gov/files/NCSC/documents/news/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021.pdf

So, organizational incident response practices must be proactive; anticipate future threats; and be looking for indicators of attacks from other vectors.[11]

- Incident response capabilities should include:
  - Cross-trained incident response personnel;
  - Multi-disciplined analysis and response capabilities;
  - Proactive monitoring and analysis across threat vectors; and
  - Generation of threat information to serve as a basis for threat intelligence.

Capabilities Required to Achieve the Intended Outcomes:

The actions, or capabilities, leaders should take to achieve the intended outcomes – the end-goal of making our high-valued assets harder targets by understanding, anticipating, and mitigating threats.

- **Ensure your organization has an enterprise-wide governance structure poised to provide enterprise-wide risk management governance AND promote proactive, blended, threat-mitigation practices (such as insider threat and OPSEC) – to achieve the aforementioned shared intended outcomes and the end-goal.[12]**
  To achieve a true, blended defense requires a top-down, leadership-driven effort – one that goes beyond traditional security programs, includes all stakeholders, and is distributed across all security domains and organizational programs.

- **Designate a principal senior official, or the equivalent, for enterprise-wide risk/threat mitigation.**
  This official must have direct access to the head of the organization AND be of sufficient rank to be in the chain of command for all threat/risk mitigation practices.

- **Establish an enterprise-wide risk management council, advisory board, or the equivalent.**
  This senior-level body supports the head of your organization and leads your organization's enterprise risk mitigation capability to proactively counter adversarial threats.
  - This body should be comprised of all program operations and mission-support stakeholders (including threat mitigation programs (such as insider threat and OPSEC), information management, human capital, financial resource management, contracting and acquisitions, legal, and other appropriate units.)
  - This body – with the designated senior official as chair – should oversee the process of identifying your organization's high-valued assets; the risk assessment process to assess vulnerabilities; and the development of strategies, policies, and procedures for mitigating and countering threats.

[11] National Institute of Science and Technology (NIST) Publication 800-53, Rev 5, *"Assessing Security and Privacy Controls for Information Systems and Organizations."* This publication includes numerous controls for incident response, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[12] OMB Circular 123, 2016 revision, *"Management's Responsibilities for Enterprise Risk Management and Internal Control."* This publication describes Enterprise Risk Management Councils and notes they should be chaired by a senior official with responsibility for the enterprise. The circular notes this should be the Deputy Secretary in cabinet-level agencies. https://www.whitehouse.gov/sites/files/omb/memoranda/2016/m-16-17.pdf

Recommended Actions:

1. **Refine your understanding of Enterprise Risk Management** as outlined in the Office of Management and Budget (OMB) Circular 123 *"Management's Responsibilities for Enterprise Risk Management and Internal Control."*

2. **Refine your understanding of Operations Security (OPSEC)** and the "cycle" described in National Security Presidential Memorandum (NSPM) 28 "The National Operations Security Program (NOP)"

3. **If not already underway, bring together the security elements within your organization *(as identified in OMBC 123)* to begin the dialogue** about how your organization approaches and understands the threats you face – and the risks associated with those threats.

4. **Advocate for a governance structure** dedicated to collectively identifying your organization's high-valued assets and the measures required to counter and mitigate threats to those assets.

5. **Recommend your agency head designate a senior official to lead this governance structure and establish an enterprise-wide risk management council, or advisory board, responsible for oversight.** Your senior official for risk management could be the same as the one designated for your Insider Threat Program, or your director of security. You don't have to create a new position, perhaps just modify current organizational structures and align risk management responsibilities and accountability where it makes sense for your organization.

6. **Explore your organization's capability for generating and/or obtaining threat intelligence specific to your mission and high-valued assets.** NSPM-28 specifically states that "Agencies with access to classified information and insight into OPSEC threats shall support other agencies without such access by identifying Critical Information that may be of use to an adversary, providing analysis of risks associated with external threats to Critical Information[13], recommending or implementing appropriate countermeasures, and other appropriate information sharing."

7. **Engage with your strategic communication or public affairs colleagues to communicate, communicate, and communicate – with the entirety of your organization.** Build the culture of security, trust, inclusion, and mutual-understanding of the threats you face. Build the groundswell of support and a call to action from your entire workforce getting their buy-in and participation in this process. Your workforce cares about your mission and they are proud of what they do and your mission. They will grow to view your high-valued assets as their own and will be eager to protect them. Put them to work, as partners, in your risk management process.

[13] Critical Information definition: Classified or unclassified information important to the achievement of U.S. objectives and missions that requires safeguarding or dissemination controls and for which unauthorized access to, or modification of, could adversely affect the national interest or national security, the conduct of Federal programs or operations, or individual privacy and Identity Management. National Security Presidential Memorandum (NSPM) 28, "*The National Operations Security (OPSEC) Program,*" January 13, 2021, JWICS site: https://www.ncsc.ic.gov/etd/docs/NCSC-21-00137_Memo_National_Operations_Security_Program.pdf.pdf

In support of this effort, the NCSC Enterprise Threat-Mitigation Directorate (NCSC/ETD) will continue to work with departments and agencies across the federal government to help develop and refine these capabilities.

Included below is a handout to supplement this narrative and a detailed list of threat mitigation resources for reference.

For more information, please email the NCSC/ETD at NITTF-Assitance@dni.gov or on JWICS at ETD_Assistance.wma@cia.ic.gov.

Robert W. Rohrer
Assistant Director, Enterprise Threat-Mitigation Directorate
Director, National Insider Threat Task Force
National Counterintelligence and Security Center

Threat Mitigation Resources

U.S. Federal Government Policies and Authorities		
Privacy Act	The Privacy Act of 1974 – https://www.justice.gov/opcl/privacy-act-1974	1974
EO-12333	United States Intelligence Activities https://www.archives.gov/federal-register/codification/executive-order/12333.html	1981
EO-12829	National Industrial Security Program https://www.archives.gov/files/isoo/policy-documents/eo-12829.pdf	1993
EO-12968	Access to Classified Information https://www.govinfo.gov/content/pkg/FR-1995-08-07/pdf/95-19654.pdf	1995
EO-12977	Interagency Security Committee https://www.govinfo.gov/content/pkg/FR-1995-10-24/pdf/95-26497.pdf	1995
EO-13526	Classified National Security Information https://www.archives.gov/isoo/policy-documents/cnsi.co.html	2009
EO-13549	Classified National Security Information Programs for State, Local, Tribal and Private Sector Entities https://www.federalregister.gov/documents/2010/08/23/2010-21016/classified-national-security-information-program-for-state-local-tribal-and-private-sector-entities	2010
EO-13556	Controlled Unclassified Information (CUI) https://www.govinfo.gov/content/pkg/FR-2010-11-09/pdf/2010-28360.pdf	2010
EO-13587	Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information https://www.archives.gov/files/isoo/policy-documents/co-13587.pdf	2011
EO-13636	Improving Critical Infrastructure Cybersecurity https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity	2013
Counterintelligence Enhancement Act	Counterintelligence (CI) Enhancement Act of 2002 https://www.dni.gov/files/NCSC/documents/Regulations/CI_Enhancement_Act_of_2002.pdf	2002
National Insider Threat Policy and Minimum Standards	National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs https://www.dni.gov/files/NCSC/documents/nittf/National_Insider_Threat_Policy.pdf	2012
Insider Threat Mitigation Guide	Insider Threat Mitigation Guide for U.S. Critical Infrastructure Entities https://www.dni.gov/files/NCSC/documents/nittf/20210319-Insider-Threat-Mitigation-for-us-critical-infrastru-march-2021update-5apr21b.pdf	2021
NSPM-28	National Security Program Memorandum "The National Operations Security Program (NOP) JWICS site: https://www.ncsc.ic.gov/etd/docs/NCSC-21-00137_Memo_National_Operations_Security_Program.pdf.pdf	2021
OMB Circular-123	Management's Responsibility for Enterprise Risk Management and Internal Control https://www.whitehouse.gov/sites/files/omb/memoranda/2016/m-16-17.pdf	2016
OMB Memo 19-03	Strengthening Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program https://www.whitehouse.gov/wp-content/uploads/2019/03/M-19-13.pdf	2018

OMB Circular A-130	Managing Federal Information Resources https://obamawhitehouse.archives.gov/omb/circulars_a130_a130trans4	2000
FISMA (2002)	Federal Information Security Management Act (FISMA) https://www.congress.gov/bill/107th-congress/house-bill/3844	2002
FISMA (2014)	Federal Information Security Modernization Act (FISMA) https://www.congress.gov/bill/113th-congress/senate-bill/2521	2014
NIST RMF	National Institute of Standards and Technology (NIST) *"Risk Management Framework (RMF)"* https://csrc.nist.gov/Projects/risk-management/about-rmf	2021
NIST 800-39	National Institute of Standards and Technology (NIST) *"Managing Information Security Risk: Mission and Information System View"* https://csrc.nist.gov/publications/detail/sp/800-39/final	2011
NIST 800-53	National Institute of Standards and Technology (NIST) *"Security and Privacy Controls for Information Systems and Organizations"* https://csrc.nist.gov/privacy-framework/nist-sp-800-53	2020
NIST 800-53.A	National Institute of Standards and Technology (NIST) *"Assessing Security and Privacy Controls for Information Systems and Organizations"* https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final	2022
SEAD-1	Security Executive Agent Directive 1 – *"Security Executive Agent Authorities and Responsibilities"* https://www.dni.gov/files/NCSC/documents/Regulations/SEAD_1.pdf	2012
SEAD-3	Security Executive Agent Directive 3 – *"Reporting Requirements for Personnel With Access to Classified Information or Who Hold a Sensitive Position"* https://sgp.fas.org/othergov/intel/sead-3.pdf SEAD-3 Toolkit: https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/sead-3-toolkit	2017
SEAD-4	Security Executive Agent Directive 4 – *"National Security Adjudicative Guidelines"* https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf	2017
SEAD-5	Security Executive Agent Directive 5 – *"Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications"* https://www.dni.gov/files/NCSC/documents/Regulations/SEAD_5.pdf	2016
SEAD-6	Security Executive Agent Directive 6 – *"Continuous Evaluation"* https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-6-continuous%20evaluation-U.pdf	2018
PDD-12	Presidential Decision Directive 12 – "Security Awareness and Reporting of Foreign Contacts" https://irp.fas.org/offdocs/pdd/pdd-12.pdf	1993
NSTISSD No. 501	National Training Program for *"Information Systems Security (INFOSEC) Professionals"* https://www.cnss.gov/CNSS/openDoc.cfm?8LkOjdlnYV1MH2Cen64ypw==	1992
CNSSD No. 502	Committee on National Security Systems Directive on *"Security of National Security Systems"* https://www.cnss.gov/CNSS/openDoc.cfm?xvnFBaMTm2pASKXL9YOvsA==	2004
CNSSD No. 505	Committee on National Security Systems Directive on *"Supply Chain Risk Management"* https://www.cnss.gov/CNSS/openDoc.cfm?RNCMDzJDXXD1qy3r9eKmugg==	2021
CNSSI No. 4009	Committee on National Security Systems Instruction *"Glossary"* https://www.dnss.gov/CNSS/openDoc.cfm?nlpeHdTd15WNb/cCDa97qA==	2022

U.S. Intelligence Community (IC) Publications		
Intro to the IC	Introduction to the U.S. Intelligence Community, 2020-2021 JWICS site: https://intelshare.intelink.ic.gov/sites/icoverview/SitePages/ICOverview.aspx	2022
ICD-700	Protection of National Intelligence – https://www.dni.gov/files/documents/ICD/ICD_700.pdf	2012
ICD-701	Unauthorized Disclosures of Classified National Security Information https://www.dni.gov/files/documents/ICD/ICD_701.pdf	2017
ICD-702	Technical Surveillance Countermeasures https://www.dni.gov/files/documents/ICD/ICD_702.pdf	2008
ICD-703	Protection of Classified National Intelligence (CNI) including Sensitive Compartmented Information (SCI) – https://www.dni.gov/files/documents/ICD/ICD_703.pdf	2018
ICD-704	Personnel Security Standards and Procedures for Access to SCI https://www.dni.gov/files/documents/ICD/ICD_704.pdf	2018
ICD-705	Sensitive Compartmented Information Facilities (SCIFs) https://www.dni.gov/files/documents/ICD/ICD_705.pdf	2010
ICD-706	Security Standards for Protecting Domestic IC Facilities https://www.dni.gov/files/documents/ICD/ICD_706.pdf	2016
ICD-731	Supply Chain Risk Management (SCRM) – https://www.dni.gov/files/documents/ICD/ICD_731.pdf	2013
ICD-750	Counterintelligence Programs – https://www.dni.gov/files/documents/ICD/ICD_750.pdf	2013

Other Resources	
National Counterintelligence and Security Center (NCSC)	https://www.dni.gov/index.php/ncsc-home
National Insider Threat Task Force (NITTF)	https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf
DCSA's Center for Development of Security Excellence (CDSE) Toolkits for: Unauthorized Disclosure, Information Security, Counterintelligence, and Insider Threat Toolkit	https://www.cdse.edu/
Defense Personnel and Security Research Center (PERSEREC)	https://www.dhra.mil/perserec/
National Institute of Standards and Technology (NIST) NIST Publications	https://www.nist.gov/ https://www.nist.gov/publications
Controlled Unclassified Information (CUI)	https://www.archives.gov/cui
OMB Circular – 123 – Management's Responsibility for Enterprise Risk Management and Internal Controls	https://www.whitehouse.gov/sites/files/omb/memoranda/2016/m-16-17.pdf
Interagency OPSEC Support Staff (IOSS) *(Realigned under National OPSEC Program (NOP), NCSC/ETD*	https://www.ioss.gov

ENTERPRISE THREAT MITIGATION

A new way of understanding how to mitigate the growing scope and magnitude of the adversarial threat to our nation using an organization-wide, capabilities-driven framework.

Framework

Blended Defense

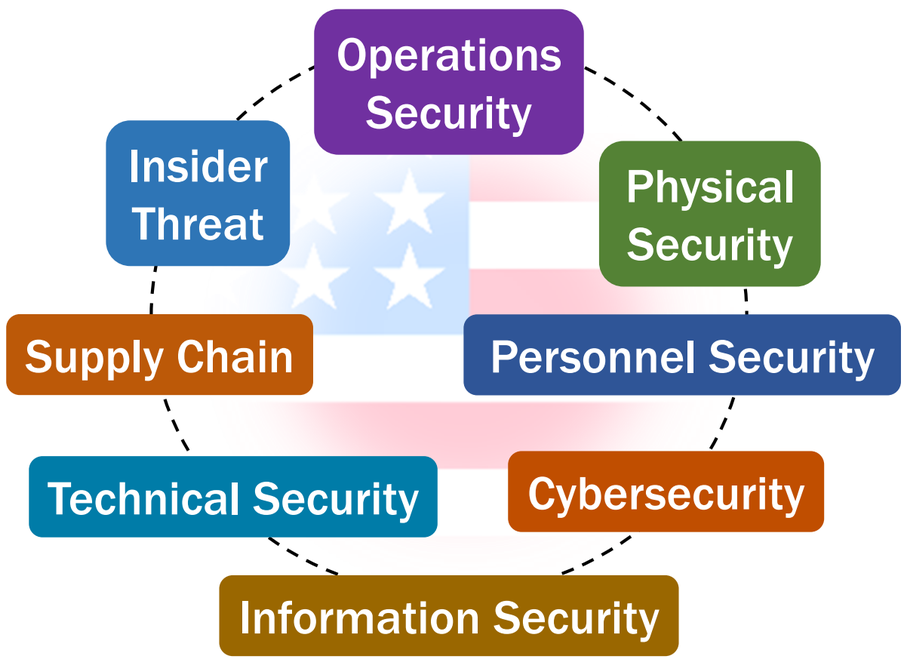
A blended defense to counter the blended offense of sophisticated competitors.

Threat Intelligence

Organizations build and maintain a threat intelligence capability.

Proactive Response

Organizations have proactive, coordinated incident response practices.



High-Value Assets

Threats to high-value assets are included in all risk management practices on an enterprise level.

Understand the Threat

Every employee – from upper management to entry-level – understands the risk the organization faces from adversarial threats.

Model for Building a Framework

Establish an enterprise-level risk council or board

- Comprised of all program operations and mission-support stakeholders
- Leads the organization's enterprise risk mitigation capabilities

Ensure enterprise-wide governance

- Council/Board and senior official provide governance
- Promotes proactive, blended threat-mitigation practices

Designate a principal senior official

- Chairs the risk council or board
- Responsible for all threat mitigation practices
- Direct access to organization head

To Do

- ✓ Take stock of enterprise-wide risk posture
- ✓ Identify high-value assets
- ✓ Identify all paths to high-value assets
- ✓ Understand adversarial capabilities and intent
- ✓ Understand adversarial valuing of assets
- ✓ Ensure enterprise-wide capability to observe, anticipate, document, and counter threat-vector changes
- ✓ Identify resource needs and shortfalls