OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY

OFFICE OF THE DIRECTOR FOR DEFENSE INTELLIGENCE

(COUNTERINTELLIGENCE, LAW ENFORCEMENT, AND SECURITY)

DEFENSE SECURITY ENTERPRISE STRATEGY

FY2021-2025

LAST UPDATED

July 2021

AUTHORED BY

Garry Reid, Director for Defense Intelligence, CL&S

Tara Jones, Deputy Director for Defense Intelligence, CL&S


Petty Officer 2nd Class William Sykes

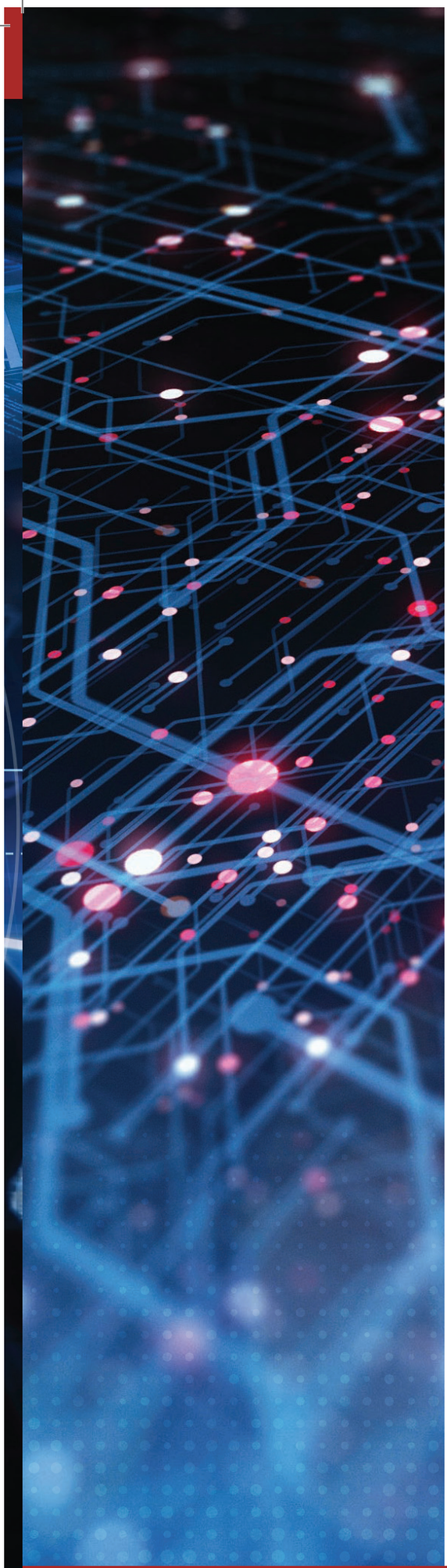


TABLE OF CONTENTS

MESSAGE FROM THE DEFENSE SECURITY EXECUTIVES

We are pleased to present the Defense Security Enterprise (DSE) Strategy for Fiscal Years (FY) 2021-2025. This strategy, developed collaboratively across the Enterprise, provides a framework for the DSE as we seek to elevate, integrate, and optimize Defense Security in a formidable threat environment.

This Strategy outlines the goals and objectives for the Enterprise to pursue for a more cohesive, integrated, and future-focused security framework. Overcoming traditional silos and addressing critical gaps more effectively will enable the Enterprise to capitalize on commonalities, identify security gaps, and collaboratively develop solutions that improve the Nation's security.

As you familiarize yourself with the strategy, we hope you will share it with your leadership, partners, and stakeholders to foster dialogue and seek effective means of addressing the Department's most pressing security needs. We hope this strategy serves to emphasize the nature of the threats facing the United States and solidify your commitment to facing these challenges in partnership. We look forward to continued collaboration as the Enterprise coalesces around redefining and elevating security for the 21st century.

Garry Reid
Director
for Defense Intelligence, CL&S

Tara Jones
Deputy Director
for Defense Intelligence, CL&S

EXECUTIVE SUMMARY

The United States faces an unprecedented threat environment as asymmetric, non-kinetic warfare increasingly threatens critical infrastructure, undermines democratic institutions, and erodes U.S. military readiness and competitive advantage. To defend freedom, preserve economic prosperity, and maintain global stability, the Department must have an effective, efficient, and forward-looking Defense Security Enterprise (DSE).

Since the release of the 2013 DSE Strategy, the threat environment has evolved and become more complex; a robust security architecture has never been more essential to the Department's success. Strategic competitors increasingly disrupt the patterns of traditional warfare and endanger global stability in the process. As new technological capabilities embolden U.S. adversaries, the DSE must not only keep pace but anticipate new vulnerabilities and avenues of attack. Such vulnerabilities and targets may range from emerging technologies, growing reliance on the Internet of Things, dual-use intellectual property, a diffuse global supply chain, the uncleared industrial base, and controlled unclassified information.

In the face of evolving challenges, the DSE must establish and implement a robust security framework to enable cooperation and collaboration across the Enterprise. The DSE must improve and elevate the security culture within the Department and posture to maintain strategic and operational dominance against dynamic threats. To succeed, the DSE must reassess and re-engineer its methods, embrace innovation, and work with the U.S. interagency, the national security innovation base (NSIB), and allied and partner nations to effectively elevate security. The DSE will engage its partners and peers to better understand gaps in the existing security framework and the interdependencies of security-related functions. The DSE will strive to re-create or modify existing methods, better coordinate security practices among its stakeholders, increase awareness and understanding of Defense Security, share information effectively and efficiently, and define measures for success.

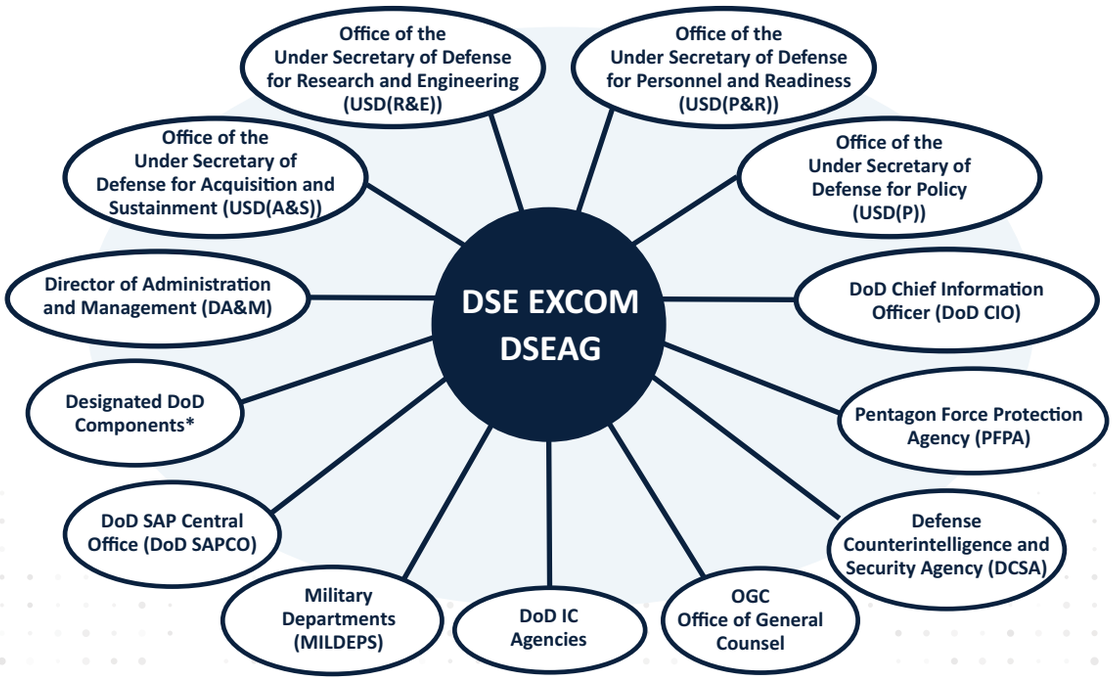
The *FY2021-2025 DSE Strategy* provides a course of action for the Department to **elevate, integrate, and optimize** Defense security. By implementing this strategy, the DSE will better align security resources across the Enterprise, enhance integration and standardization, and optimize our ability to anticipate threats and vulnerabilities. With a more robust security framework, the Department will be better equipped to combat the complex, diverse, and harmful range of threats to U.S. interests and assets.

DSE OVERVIEW

The DSE is a community with the shared mission to safeguard Department personnel, information, and property against harm, loss, misuse, or hostile acts and influences in support of national security.[1]

The Enterprise is comprised of stakeholders from across the Department and seeks to collaborate with other enterprise and national security efforts to include the intelligence community (IC) and the national security innovation base. The DSE formally convenes stakeholders through senior-level governance and leadership forums, such as the DSE EXCOM and DSEAG (see Appendix A for the full list of responsibilities for each body). Through these forums, the DSE will collaborate to achieve its vision and strategy, provide direction and solutions on issues that impact the Enterprise, measure progress toward DSE goals, and remove barriers for the good of all Enterprise stakeholders. Through integrated plans, infrastructure, and measures, the DSE EXCOM and the DSEAG will ensure a unified Defense security framework, a robust Defense Security strategy, and a comprehensive arsenal of policies to improve risk management and codify systems that safeguard Departmental resources.

DEFENSE SECURITY ENTERPRISE



1 DoD Directive 5200.43, "Management of the Defense Security Enterprise," July 14, 2020, as amended.
*Designated DoD Components to include any Components invited to participate on EXCOM meetings by the Defense Security Executive.

THE NEED FOR AN INTEGRATED ENTERPRISE

The current threat environment challenges the United States' ability to secure its workforce, operations, and position as a world leader. U.S. strategic and operational dominance has already deteriorated against a backdrop of adversarial threats of increasing speed and scope. The DSE must assess and quantify evolving security threats, reduce misalignment of effort across the Enterprise, integrate security and security-related functions, and influence departmental stakeholders to elevate security to overcome this formidable environment.

The Enterprise must work together to increase awareness of critical national security threats to inform risk management and reduction. Some of the most prominent threats to national security include:

ASYMMETRIC WARFARE FROM STRATEGIC COMPETITORS

Modernized and aggressive adversarial regimes increasingly challenge the international order and stability of democratic nations. The United States must anticipate and combat new methods of warfare and bolster partnerships with allied and partner nations to mitigate attacks on U.S. economic and political institutions. The Enterprise must posture the United States to protect a growing set of vulnerabilities, especially within the supply chain and NSIB. Through increased cooperation and understanding, the Enterprise can remain vigilant against evolving and formidable adversarial threats.

TERRORISM AND INSIDER THREATS

The Department faces multi-faceted challenges from terrorists, self-radicalized lone actors, domestic extremists, active shooters, and malicious insiders. They continue to misuse government information, target Department personnel and operations, and cause irreparable damage to critical assets. As threats evolve in nature and scale, the potential costs to national security are magnified. The Department must remain vigilant and educate its workforce on current and real threats, especially as military members are increasingly targeted by domestic terrorist groups due to their credibility and skill sets. The DSE must change the narrative surrounding the evolution of terrorists and insider threats, raise awareness around behavioral indicators, and increase reporting through interconnected tactics and solutions.¬

TECHNOLOGICAL ADVANCEMENTS

Technological advancements in fields including information communications technology (ICT); artificial intelligence (AI); nanotechnology; cybersecurity; space technology; biotechnology; and quantum computing create growing concerns for the protection of critical Department assets and information. As adversaries utilize new capabilities, the range of potential targets has increased, from mobile devices and intellectual property to weapons systems and democratic elections. The Department must keep pace with new system development to replace outdated and inferior systems. The growing vulnerability of U.S. critical technology and information systems must be central to the Enterprise's strategic operations and planning.

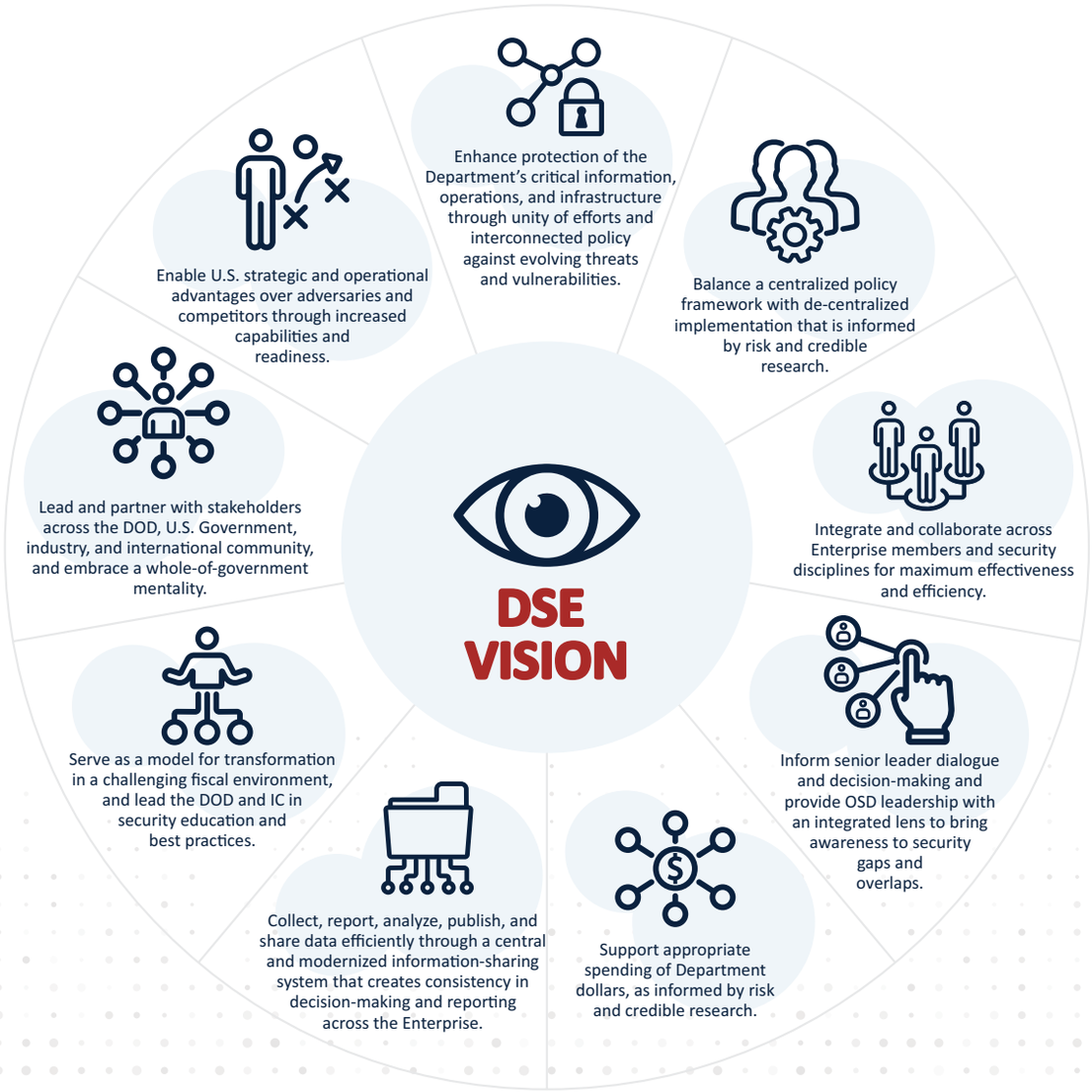
Regardless of the formidable threat environment, the United States has a unique opportunity to evolve and build the infrastructure required to maintain dominance and outmaneuver its enemies. Through collaboration, the Enterprise can improve its ability to assess the risks that pose the greatest threats to national security and prioritize resources based on those risks. Through leadership and well-executed governance, the DSE can enable world-class security approaches and modernize its workforce, processes, and policies. The DSE can create new unique and cutting-edge capabilities through partnerships with other federal agencies, government and academic research laboratories, industrial base partners, and allied and partner nations. Integrated partnerships will enable the Department to leverage additional resources and better combat current and future adversarial threats.

This DSE Strategy outlines the goals and objectives that will enable the DSE to: (1) re-conceptualize and prioritize security (elevate); (2) strengthen relationships and cohesion across the Department, the NSIB, the U.S. interagency, and with allied and partner nations (integrate); and (3) establish the infrastructure and leadership necessary to prioritize and leverage cutting-edge solutions to emerging threats (optimize). As a unified Enterprise, the DSE has the opportunity to strengthen security and shore up democratic and economic prosperity.

DSE VISION 2025

Through collaboration and coordination, the DSE will develop a more robust and integrated security infrastructure to strengthen national security by ensuring the resilience of its programs, protecting people, and safeguarding information.

In summer 2020, DSE stakeholders came together to create a shared vision of the Defense Security future state. As a result of these discussions, the DSE EXCOM committed to the following vision for the DSE in 2025:



DSE VALUES

DSE stakeholders identified the following values to guide the decisions and actions of the Enterprise as it develops and implements rigorous strategies, disciplined leadership, intentional mission management, and deliberate education.

MAINTAIN WARFIGHTING ADVANTAGE

We protect defense information, personnel, resources, and critical infrastructure and promote warfighting advantage solutions to enable the Department's mission.

LEAD WHAT'S NEXT

We generate forward-thinking solutions to stay ahead of competition and technological advancements and anticipate evolving threats.

RISK-BASED VARIATION, UNCOMPROMISED RESULTS

We apply consistent standards to our security policies and practices but provide room for variability within logic and reason.

EMBRACE A WHOLE-OF-GOVERNMENT APPROACH

We unify behind common goals and an integrated joint-warfare mentality to promote effective information sharing and maximize the benefits of collective intelligence.

DEMONSTRATE ACCOUNTABILITY AND TRUST

We improve mission execution through transparent decision-making, clear divisions of responsibility, and instilled connectivity and dialogue throughout the policy-making process.

DSE STRATEGIC GOALS AND OBJECTIVES

ELEVATE **INTEGRATE** **OPTIMIZE**

The DSE EXCOM developed three overarching goals with specific objectives to address the evolving threat environment. The EXCOM's goals and objectives guide the Enterprise to strengthen the Department's security posture and achieve the DSE vision. These goals and objectives will remain consistent throughout the duration of the DSE Strategy's lifecycle; however, DSE leadership shall revisit the initiatives used to accomplish these goals and objectives on an annual basis.

GOAL 1: ELEVATE DEFENSE SECURITY ACROSS THE DEPARTMENT, FEDERAL GOVERNMENT, AND INDUSTRY

The DSE partners with stakeholder organizations in the Department, the Federal Government, and the commercial sector to protect critical assets. To do this most effectively, stakeholders must share a common understanding about the critical role security plays in 21st century warfare, so that the Enterprise prioritizes actions necessary to secure the Department. The DSE will convey the importance of security through effective communication via targeted messaging and collaboration with its partners.

- **Objective 1.1. Empower and professionalize the security workforce to execute its mission through enhanced and standardized security education, training, and credentialing**

  DSE security workforce represent the front line of the Department's security mission. To ensure security professionals are best equipped to execute their mission, leadership must ensure their understanding of the security mission's interconnectivities and strengthen their ability to communicate how each respective discipline impacts the national security mission. The Enterprise must empower its workforce through professionalization, education, and certification programs. By equipping and training those on the front lines to effectively implement the security mission, the DSE will realize a more secure Department and consequently elevate security within the U.S. Government and across partnerships.

- **Objective 1.2. Expand the perimeter of security beyond cleared industry to external partners in the uncleared defense industrial base and NSIB**

  The range of U.S. critical assets vulnerable to adversarial threats has greatly expanded, endangering the security of the national supply chain and industrial base. Today, security risks arise early in the industrial supply chain, subjecting our research and intellectual property to potential exploitation by near-peer competitors. The DSE seeks to better protect its operations by broadening its security purview beyond the current DIB to uncleared industry and expanding partnership within the NSIB to educate industry stakeholders on growing security vulnerabilities. This expanded focus will increase awareness of the importance of security and its impact on the United States and on industry's financial and security health.

- **Objective 1.3. Influence stakeholders across the Enterprise to prioritize security in decision-making**

  The renaming of the Under Secretary of Defense for Intelligence to the Under Secretary of Defense for Intelligence and Security (USD(I&S)) was the first step toward increasing the prominence of the security mission across the Department. As leaders of the Enterprise, it is the EXCOM's responsibility to carry out this mission with excellence by driving security as a central tenet in Department decision-making, rather than as an afterthought. Through stakeholder engagement and communication, the DSE EXCOM will promote the importance of security to Defense leadership and Components and to federal organizations. Such efforts will help to ensure security credibility through increased transparency and accountability, ensuring policies are properly planned and programmed so that policy issuances are executable as written and security priorities are understood and pursued.

GOAL 2: COORDINATE POLICIES, PROCESSES, AND OPERATIONS ACROSS THE ENTERPRISE AND AMONG THE SECURITY DISCIPLINES AND SECURITY-RELATED FUNCTIONS

Enterprise stakeholders and partners must work together to reduce misalignment and wasted resources that hinder progress toward elevating security. To strengthen and standardize cross-enterprise coordination, the DSE must implement a Defense Security framework to clarify and articulate how security and security-related functions must work together. This framework will enable a consistent and integrated approach to security management and execution. Together, the Enterprise can accelerate the distribution of critical intelligence and facilitate rapid multilateral risk awareness and assessment.

- **Objective 2.1. Standardize coordination among security disciplines and security-related functions**

  The DSE will lead stakeholder organizations to create a cross-functional culture, solve problems beyond conventional means, and equip subject matter experts across the security disciplines. Today's collaborative pathways between security disciplines and security-related functions—including acquisition security, critical technology protection, counterintelligence, law enforcement, foreign disclosure, security cooperation, technology transfer, export control, nuclear physical security, chemical and biological agent security, antiterrorism, and mission assurance policy—can be improved to reduce misalignment and silos. The DSE must leverage relationships with security-related functions and clarify expectations for working together. The DSE will establish a cross-discipline framework to communicate expectations for collaboration, provide recommended processes for cross-discipline security professionals, and establish a common security lexicon from which to work.

- **Objective 2.2. Manage and centralize security information collection, reporting, analysis, and dissemination**

  Today's information-sharing systems can be improved to enable real-time analysis and dissemination, enable metric-driven decision-making, and reduce duplicative spending, collection, and reporting. The DSE will help stakeholder organizations more effectively link information and data sources from across the Enterprise through a series of centralized systems. This will enable Enterprise partners to build on one another's knowledge and security information, working toward solutions together rather than across the divide of outdated systems and processes.

- **Objective 2.3. Enable and facilitate the build-up of the Defense Counterintelligence and Security Agency's (DCSA) operational capabilities across all security domains**

  The DSE will assist DCSA to define, shape, and make progress towards the future state of DCSA to effectively execute security operations in an integrated fashion. Then, the DSE will support DCSA as necessary to achieve the DCSA mission as stated in EO 13969, and as established in the DCSA Charter, to manage security programs, conduct security operations, and integrate the security community to increase its effectiveness. Through the DSEAG and EXCOM bodies, DCSA and the DSE will work together to assess critical challenges facing the Enterprise and identify solutions so that DCSA may achieve progress towards its full operational capabilities.

GOAL 3: ESTABLISH AN INTEGRATED CAPABILITY TO ANTICIPATE AND RESPOND TO EVOLVING THREATS WITH SPEED AND INNOVATION

U.S. security infrastructure has deteriorated under the pressure of rising 21st century adversarial threats and competing national security requirements. The Enterprise must adapt and bolster its capabilities to swiftly develop and deliver new concepts, maintain a strategic and operational advantage, out-perform adversaries, and meet 21st century threats and information requirements with 21st century solutions.

- **Objective 3.1. Collect, assess, and prioritize fiscal priorities for the Enterprise to better anticipate annual budget cycles**

  The DSE faces a growing challenge to deliver at the speed of relevance while facing budget constraints. In the current fiscal environment, the Enterprise must embrace a proactive approach to budgetary planning and conduct due diligence on potential and existing security programs. This will ensure that new requirements are appropriately planned and programmed through the Planning, Programming, Budgeting and Execution (PPBE) process and Program Objective Memorandum (POM) cycle so policies and issuances are executable. By identifying and prioritizing no-fail initiatives, the Enterprise will improve its ability to anticipate and respond to evolving threats with speed and innovation despite a limited budget.

- **Objective 3.2. Utilize governance processes to oversee and manage the implementation of the DSE Strategy**

  The role of the DSE EXCOM and DSEAG is to oversee and manage the implementation of the Defense Security Strategy. To effectively oversee and manage the Strategy, DSE leadership must be able to track and measure progress. This requires follow-through of critical Enterprise-wide initiatives and assessments of performance measures and gaps. If the Enterprise is to succeed, it must define, collect, and assess key performance indicators (KPIs) that measure progress and performance toward outcomes. DSE leadership has designed a revised governance structure (see Appendix A) and will establish and implement the governance processes to achieve these objectives. This governance will drive progress toward an integrated capability across the Enterprise.

- **Objective 3.3. Conduct scientific research to identify and leverage innovative approaches to security programs and processes**

  The DSE must leverage research opportunities to innovate and integrate its current processes and systems, collaborating with cutting-edge institutions and industry partners to capitalize on U.S. technological advances and stay ahead of adversarial competition. This will increase the DSE's ability to remain future-focused and flexible in the face of evolving threats. The Applied Research Lab for Intelligence and Security (ARLIS) is a critical research partner that will inform current and future approaches to integrated security programs and processes.

CONCLUSION

DSE leadership, in collaboration with the Enterprise, developed the FY2021-2025 DSE Strategy to provide an actionable plan for the Department to elevate, integrate, and optimize security to position the nation for continued prosperity and military dominance. This effort will strengthen strategic and operational alignment, reduce misalignment and silos, and enhance capabilities to build a more robust security infrastructure. The Department and the Nation's strategic advantage depends on the success of the DSE. This Strategy is a commitment to strengthened resolve across the Enterprise to anticipate and mitigate evolving threats, promote the security mission across the U.S. Government, and ensure American resilience.

APPENDIX A: DSE GOVERNANCE

DEFENSE SECURITY ENTERPRISE EXECUTIVE COMMITTEE (DSE EXCOM)

The DSE EXCOM is the senior-level forum comprised of Tier-3 civilian executives or three-star GO/FO directors or equivalent representatives from the Military Departments, select Department Components, and Fourth Estate organizations. The EXCOM collaborates across traditional organizational boundaries to establish and measure DSE strategic direction and provide cross-discipline perspectives to strengthen the Defense security posture. The primary responsibilities of the DSE EXCOM include:

Lead

The EXCOM sets the strategic direction for Enterprise-wide security policy and high-impact security decisions. It approves and updates the DSE vision, responding to the changing threat environment, and approves the DSE Strategy to achieve the vision. Along the way, the EXCOM identifies and removes barriers to success.

Advise

The EXCOM assesses, prioritizes, and endorses critical DSE decisions and initiatives. It utilizes the DSEAG to conduct due diligence on priority initiatives through working groups, then evaluates the working groups' findings. After thorough assessment, the EXCOM agrees to course corrections for priority initiatives.

Oversee

The EXCOM identifies, monitors, and refines KPIs to measure and monitor progress against the DSE Strategy. It assesses performance to focus on gaps or underperforming areas and to evaluate the effectiveness of critical Enterprise initiatives.

DEFENSE SECURITY ENTERPRISE ADVISORY GROUP (DSEAG)

The DSEAG is the operational arm of the DSE, comprised of Tier-2 civilian executives or two-star GO/FO deputy directors or equivalent representatives from the Military Departments and select Department Components, as well as Fourth Estate organizations. The DSEAG assesses the objectives, risks, and pressing issues facing the Enterprise to make recommendations and escalate decisions to the EXCOM. The primary responsibilities of the DSEAG include:

Collect & Qualify

The DSEAG surfaces and prioritizes critical initiatives from Components' security organizations to elevate to the EXCOM. These initiatives must have a direct impact on DSE member organizations, relate to DSE strategic goals, require cross-enterprise perspectives, and/or require further assessment and oversight to enable success. Once an initiative is identified and prioritized, the DSEAG conducts a rapid assessment or launches a working group to prepare recommendations on a path forward.

Manage

As the standing support body to the EXCOM, the DSEAG escalates decisions, prepares briefs, and documents EXCOM decisions and recommendations. The DSEAG is the coordinating body for security program reviews and prioritizes and deconflicts resources for the security community to ensure an integrated and mutually reinforcing Enterprise. The DSEAG also staffs, launches, and oversees DSE working groups, providing a consistent approach and set of best practices. The DSEAG leverages working groups as finite entities that work to solve a specific problem for a pre-determined amount of time. It evaluates working group assessments and findings before preparing EXCOM members for decisions.

Analyze & Report

The DSEAG consolidates and analyzes KPI data across the Enterprise to determine whether there are shortfalls in a program's implementation. The DSEAG also briefs the EXCOM on security performance measures and identifies critical gaps for EXCOM evaluation and decision.

APPENDIX B: DEFINITIONS

Defense Security Enterprise (DSE): The organizations, infrastructure, and measures (to include policies, processes, procedures, and products) in place to safeguard Department personnel, property, information, and mission against harm, loss, or hostile acts and influences. This system of systems comprises cyber, industrial, information, personnel, physical, and operations security, as well as SAP security policy, critical technology protection, counter insider threat, critical program information protection policy, security professionalization, and security training. It addresses, as part of information security, classified information (including sensitive compartmented information and Atomic Energy Act information) and controlled unclassified information. The DSE aligns to counterintelligence, law enforcement, foreign disclosure, security cooperation, technology transfer, export control, nuclear physical security, chemical and biological agent security, antiterrorism, acquisition security, and mission assurance policy. DSE policy is informed by other security-related efforts.

Defense Security framework: The structure or architecture behind the relationships and interactions of security disciplines.

Industrial security: A multi-disciplinary security program concerned with the protection of classified information developed by or entrusted to U.S. industry.

Information security: The system of policies, procedures, and requirements established in accordance with EO 13526 to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public pursuant to Executive order, statute, or regulation.

Insider threat: A person with authorized access who uses that access, wittingly or unwittingly, to harm national security interests and/or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions that result in the loss or degradation of resources or capabilities.

National security innovation base (NSIB): The U.S. network of knowledge, capabilities, and people—including academia, national laboratories, and the private sector—that turns ideas into innovations, transforms discoveries into successful commercial products and companies, and protects and enhances the American way of life.

Operations security: A security discipline that identifies critical information and analyzes friendly actions attendant to military operations and other activities to:

- Identify those actions that can be observed by adversarial intelligence systems.
- Determine indicators and vulnerabilities that adversarial intelligence systems might obtain and interpret (or piece together) to derive critical intelligence, then determine which of these represent an unacceptable risk.
- Select and execute countermeasures that eliminate or reduce to an acceptable level the risks to friendly actions and operations.

Personnel security: The security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility to access classified information or be assigned to sensitive positions.

Physical security: The security discipline concerned with physical measures designed to: (1) protect personnel; (2) prevent unauthorized access to equipment, installations, material, and documents; and (3) safeguard them against espionage, sabotage, damage, and theft.


DEFENSE SECURITY ENTERPRISE
DEPARTMENT OF DEFENSE
DSE