Defense Security Service
Strategic Plan **2020**

Our Agency, Our Mission, Our Responsibility

Daniel E. Payne
Director

James J. Kren
Deputy Director

Troy L. Littles
Chief of Staff

Letter from the Director

The 21st-century threat environment is enduring and persistent. I believe the United States is currently facing a counterintelligence threat that is unprecedented in our history. This increased threat is a result of advances in technology (primarily cyber and science), and the globalization of business and the American workforce. The nation is losing significant amounts of technology and information, most of which is unclassified. Further contributing to the challenge, the collection methods of our adversaries are constantly changing. To meet this new threat, DSS is changing the way it does business. In order to succeed against our adversaries, each of us, along with our industry partners, must embrace change in order to counter the evolving threat

Since becoming the DSS Director in March 2016, I have been highly encouraged by the people, performance, and progress of DSS. During my visits to the field, I have seen first-hand the quality and tremendous value of what you do every day. DSS has a robust four-decade history — and this agency continues to evolve and adapt to new mission sets, as well as an increasingly complex and dynamic security environment. Striving toward 2020 and beyond, I wholeheartedly support the mission, goals, and objectives of Strategic Plan 2020 which is in line with our agency's performance goals . I applaud the progress DSS has achieved since the inception of the plan. I also think it is important to continue to build on our foundational priorities of People First, Mission Always; and a true partnership with industry.

Shortly after I took the helm of DSS, I issued additional priorities which I believe the Strategic Plan will help us to achieve. These priorities include: workforce development; developing and instituting a risk-based approach; operational capability of the DoD Insider Threat Management and Analysis Center; transformation of the defense security enterprise; and strengthening information technology and cybersecurity. You can read more about these priorities in my 2016 Annual Guidance.

The success of our mission is dependent upon the dedication of the DSS workforce, the commitment our government customers, and continuing a strong partnership with industry. It is imperative that we remain focused, aligned, and agile, while strengthening our methods of operation as we move forward. As a firm believer in integration, collaboration, and transparency, I am looking forward to the road ahead and have every confidence that we are moving in the right direction.

Daniel E. Payne

W.C
BRYANT

Introduction & Overview

Who We Are

Under the Department of Defense (DoD), the Defense Security Service (DSS) is an agency that has supported national security for over 40 years. Established in 1972, DSS was originally created to provide a more efficient and effective personnel security investigation process; however, the agency has seen its mission and responsibilities evolve over the years as it continues to play an integral role in ensuring national security.

In 1980, the DSS mission expanded to include administration of the Defense Industrial Security Program (DISP), covering industrial contractor facility clearances, industrial personnel security, safeguarding of classified information, and physical security for all DoD contractors involved with classified material. As the agency continued to grow, new processes and programs were introduced, which included changes to personnel security investigations and the institution of periodic investigations on personnel with access to top secret information.

In response to changing environmental demands, in 1993, the agency established a counterintelligence office and moved forward with providing threat data within the agency and to industry. Also in 1993, President Bush signed Executive Order 12829, the National Industrial Security Program (NISP). Working between government and industry, the NISP was established to safeguard classified information held by contractors, licensees, and grantees of the United States Government.[1]

DSS is charged with administering the NISP for DoD and other government agencies. The NISP was followed by creation of the NISP Operating Manual (NISPOM) in 1995, which established standard procedures, requirements, and safeguards related to protecting classified information.[2]

Over the past few decades DSS has continued to adapt and adjust to the complexities that emerge in the security environment, shifting its mission and structure to accommodate

[1] Executive Order 12829, "National Industrial Security Program," January 1993.

[2] DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 2006, Incorporating Change 1, 28 March 2013.

and fully support its customer base. In 2005 the responsibility for personnel security investigations was transferred to the Office of Personnel Management (OPM). The agency continues to provide a wide range of security products and services, including security assessments, risk mitigation, and research studies, along with security training, education, and professional development to the DoD, government, and industry.

Today, pursuant to DoD Directive 5105.42,[3] DSS receives authority and direction from the Under Secretary of Defense for Intelligence and is headquartered in Quantico, Virginia. With four regional offices and 45 field offices across the Nation, DSS provides the military services, defense agencies, 27 federal agencies, and approximately 13,500 cleared contractor facilities with security support services and education.

In accomplishing its mission, DSS is comprised of four mission directorates supported by various enabling elements. The directorates include Industrial Security Field Operations (IO), Industrial Security Integration and Application (IP), Counterintelligence (CI), and the Center for Development of Security Excellence (CDSE). With the agency's unique set of capabilities, DSS will continue to serve the Nation and support national security into the future.

[3] DoD Directive 5105.42, "Defense Security Service (DSS)," August 3, 2010, Incorporating Change 1, March 31, 2011.

Strategic Planning Methodology

The DSS Strategic Plan 2020 does not exist in isolation from the broader national and DoD community. It is influenced by and aligned with many of the themes found in key documents such as:

- National Security Strategy, *May 2010*
- National Intelligence Strategy, *September 2014*
- Quadrennial Defense Review, *March 2014*
- Defense Security Enterprise Strategic Plan, *2013*

Following the format in the Office of Management and Budget (OMB) Circular A-11,[4] the DSS Strategic Plan 2020 is a dynamic document that defines the agency mission and provides a road map of five strategic goals to successfully accomplish that mission in the future. In the context of current and strategic trends, the DSS Strategic Plan 2020 provides 21 nested and integrated strategic objectives that enable the agency to accomplish each of the strategic goals.

To ensure that the Plan is dynamic and responsive to future change but also actively implemented and monitored, specific performance goals for each strategic objective, along with their associated metrics and measures, have been coordinated and approved by DSS leadership. While performance goals are not included as part of this publication, they form the backbone of the DSS Annual Implementation Plan. Their execution is assigned to appropriate offices within the agency and their performance is tracked and reported by the DSS Strategic Management Office.

The strategic plan guides development of the DSS Annual Implementation Plan and the annual Director's Strategic Planning Guidance (SPG). The SPG provides guidance and sets agency priority goals for the coming year while the Implementation Plan, which includes the SPG, establishes how DSS will work toward accomplishing the strategic goals, objectives, and performance goals of the DSS Strategic Plan.

[4] OMB Circular No. A-11, "Preparation, Submission, and Execution of the Budget," 2014.

Our Stakeholders

The agency's stakeholders are integral to DSS' success. This includes the DSS workforce, cleared industry, government agencies, the intelligence and security communities, and the Nation.

STAKEHOLDER	IMPACT
DSS Workforce	The agency's most critical asset is its people. DSS will continue to invest in growing and developing its workforce in an inclusive and professional working environment.
Cleared Industry	DSS provides oversight and assistance to cleared contractor facilities, ensuring the protection of U.S. and foreign classified and sensitive information and technology.
Government Agencies	DSS administers the NISP on behalf of the DoD and 27 other federal agencies.
Intelligence & Security Communities	Through collaboration and partnership with the larger intelligence and security organizations, DSS seeks to enhance national security.
The Nation	As a critical link between industry and the government, DSS contributes to national security for the common good of the Nation.

Mission, Vision & Values

Mission

The Defense Security Service (DSS) strengthens national security at home and abroad through our security oversight and education operations. DSS oversees the protection of U.S. and foreign classified information and technologies in the hands of cleared industry under the National Industrial Security Program by providing professional risk management services. As Functional Manager for the Department of Defense (DoD), DSS provides security education, training, certification, and professional development for the DoD and for other U.S. Government personnel, contractor employees and representatives of foreign governments.

DSS is a small agency with a unique mission and tremendous responsibility. We provide security training and certification for both industry and government agencies and provide security oversight to cleared industry.

Although serving distinct functions, the dual missions also complement one another. DSS teaches, advises, and educates security professionals, and they in turn apply what they learn and keep our Nation's and partner nation's secrets safe. Simultaneously, others in DSS provide oversight to ensure that our information remains secure both here and abroad.

Vision

Through partnership and innovation, safeguard our Nation's interests as the premier provider of industrial security risk management and security professional development services.

DSS does not stand alone in its efforts to support national security, we have numerous partners in both government and industry. Through our partnerships we form a strong bond of mutual respect and dedication to safeguarding our Nation's interests.

With our partners' assistance, cooperation, and collaboration, we provide industrial security risk management and are constantly researching and innovating to ensure that the security training and certification we provide is the best available in both content and delivery. While fulfilling our mission, we seek to be the premier provider of our services.

Values

Dependability

We are reliable, providing consistent, timely, and exceptional behavior and results on a daily basis. Our stakeholders and industry partners count on us and we seek to deliver on our obligations and be available when needed in order to demonstrate our commitment and establish trusting relationships.

Respect

We embrace an environment where every person is valued and treated fairly, and where diversity is viewed as a strength. We strive to create and maintain a reputation for mutual respect that inspires trust, confidence, and honest communication.

Integrity

We are honest and ethical, take pride in what we do, and strive to maintain an environment of mutual trust through moral conduct. There is no situation or circumstance that allows us to compromise our high standards.

Agility

We are willing and able to quickly recognize and adapt to change. We proactively seek improvement and have an insatiable appetite to continually learn and grow. We are empowered to respond to problems, challenges, and opportunities — both anticipated and unforeseen.

Collaboration

We rely on each other to work effectively, leverage diverse expertise, and cooperatively produce the best outcomes. We value our partnerships and mutual respect and trust. Teamwork is critical to who we are and what we do.

Accountability

We accept responsibility for our work and the consequences of our choices. We are competent in our actions and strive to use our expertise to make effective and efficient decisions. Personal performance is measured against achievement of the agency's strategic goals and ultimately impacts our success.

Strategic Environment

The world is rapidly changing with new technologies, emerging threats, and increased complexity and uncertainty. Within this world, many elements are at work shaping the future environment in which DSS will operate. From a constrained fiscal environment to the evolving nature of threats, from technological advancements to global realignment and data centralization, several factors will impact DSS and its mission. Identifying and understanding trends today will help DSS prepare for the future and support national security for many years to come.

The World: What Does It Look Like?

Rapid Change. The world will continue to change at a rapid pace, requiring government and industry alike to make swift adjustments in response. Today's global, technology-oriented environment compels organizations to be open to new ideas, to swiftly adapt to shifting situations, to handle unexpected demands, and to be willing and able to change strategy in order to remain relevant.

Globalization. The world has become more globally interdependent and as relationships and influences integrate further, National defense and industry must be able to sort through the complexity of international supply chains. Cleared contractors today are globally-oriented and work with a range of entities to include foreign contacts, businesses, and governments. Finding and maintaining transparency within this interconnected environment will prove to be a continuing challenge.

New Alliances. United States relationships with traditional allies are changing and may have unforeseen impacts on National security and economic interests. New and changing relations around the globe may present both challenges and strategic opportunities. Shifting alliances may expose unforeseen partnerships that involve potential adversaries or present other security concerns.

Government Security Agencies: What Are They Facing?

Fiscal Uncertainty. Underlying the entire threat environment are persistent budget constraints and unforeseen work interruptions that affect both government and industrial security stakeholders. Agencies are increasingly expected to do more with less. Under such

constraints, establishing efficiencies and adapting to the constrained environment without jeopardizing agency goals is a challenge faced by many organizations.

Complexity. An environment driven by globalization and the increased speed, quantity, and reach of human interaction will continue to increase complexity as technology diffuses power to more and more divergent groups. Balancing that complexity and safeguarding against attacks to infrastructure while exploring opportunities to share information securely will prove to be a major challenge.

Data Collection and Centralization. Intelligence, information, and data has become increasingly centralized and consolidated. Although centralized data systems can be faster to access and relatively easier to secure, they are inherently vulnerable as a single source. The magnitude of any security compromise or issue is increased in a centralized and consolidated environment. Furthermore, amidst efforts to combat threats and ensure national security, increasing amounts of personal data are being collected. There are growing societal concerns about personal data collection, the safeguarding of that data, and the adverse impact of a data breach.

Cloud Migration. Moving critical systems into virtual shared infrastructures changes how information security and risk management are addressed. Security processes and solutions are still being developed for cloud-based infrastructures, posing a challenge to maintain a secure network of information while keeping up with emerging technology. Distributed denial of service attacks are expected to be on the rise as the move to virtual servers

increases, resulting in ultra-high bandwidth events. Compared with the computer-based, lower-bandwidth attacks, this new attack vector becomes even more critical for security experts to consider as more traffic is directed through the cloud.

Technological Advancements. While technology can enable threats, it also offers opportunities for countering threats and sharing information when proper security procedures are followed. Security agencies will be challenged to determine the appropriate balance between using technology and maintaining a secure environment.

Acquisition. The gap between the current acquisition process and the need for improved security procedures further increases the potential for damage to national security. The acquisition process is highly complex and encompasses elements such as design, testing, deployment, sustainment, and eventual disposal. Acquired products need to be secured early and throughout each stage of the acquisition process. With increased fiscal constraints and pressure to accelerate acquisition processes, managing security within that process becomes increasingly challenging.

The Threat: Where Is It Coming From?

Across the Globe. The threats that impact the DoD and the national industrial security base have evolved over the past several years. Worldwide, the likelihood of instability and disorder in an increasingly unpredictable and complex security environment is ever-present and growing. Hybrid threats are increasingly common and consist of an amalgamation of criminals, drug organizations, terrorists, and rogue states working together in ad hoc, informal, or formal alliances. Combined with the diversity of stakeholders involved, these interrelated elements further complicate the threat environment and will continue to do so into the foreseeable future.

Insiders. One focus area inspired by events over the past several years is insider threat. Demand for sensitive information continues to increase and transmitting information has only become easier; consequently, threats from insiders, or trusted people within an organization, has grown. The grave damage and negative impact to national security and industry that can be caused by insiders is leading to new and enhanced precautionary measures. Many organizations have increased their use of internal monitoring and shifted towards heightened scrutiny of potential behavioral indicators; a dissatisfied employee provides a means for

enacting a detrimental or destructive insider security event. Acquisition and contractor screening processes will also become more stringent.

Cyber. Advancements in technology and increased availability of online and network capabilities have given rise to growing cyber espionage. Businesses, governments, and individuals are often targeted, compromising sensitive and critical information, data, systems, infrastructure, and other areas. Mobile security, supply chains, cloud data, and attack capability trends present issues that will continue to impact the operating environment. Coupled with increased cyber capabilities is the growing threat of intellectual property crime. With the proliferation of digital technologies, vastly improved storage device capacity, and Internet file sharing, years of work and millions of dollars of American research and development can be stolen. With comparatively minimal investment, adversaries can present a real threat to sensitive or classified U.S. intellectual property and cleared personnel.

Conclusion

Worldwide, the likelihood of instability and disorder in an increasingly unpredictable and complex security environment is ever-present and growing. Consequently, the future strategic environment presents many challenges for DSS. However, identifying and understanding trends today will help DSS prepare for the future. By planning strategically and identifying forward-thinking goals and objectives, DSS can be ready and able to address environmental concerns and support national security for many years to come.

Goals & Objectives

The DSS Strategic Plan 2020 consists of five strategic goals along with 21 supporting strategic objectives. During the life cycle of this plan, it will be continually reviewed and adjusted as needed based on the changing environment, new security law and policy, and other strategic planning developments that necessitate new direction and targets.

These five goals have been identified as critical for positioning the agency for continued effectiveness and success in the future.

Goal 1: Strengthen capabilities to continually identify, evaluate, and mitigate risk to the DoD and the national industrial base

DSS fills a unique niche in supporting the DoD responsibility for projecting U.S. power as one of the Nation's ways of maintaining security. During the first 42 years of DSS' existence, there were occasions that demanded exceptional agility and adaptability by the entire organization to transform itself, its mission performance, and even elements of the mission itself to continue filling that niche.

Looking ahead, DSS expects to again face a time of remarkable transformation. Successful accomplishment of our mission requires constant awareness of and adjustment to the changing security environment. Future success also requires proactive input to and planning for the emergence of new national and DoD security guidance. DSS will focus on ways it can best position itself to mitigate the risks faced by cleared industry and our security professionals to ensure the protection of our Nation's valuable technology, information, and warfighting capabilities.

Objective 1.1: Assess, analyze, and continuously enhance DSS' approaches to risk management

A mindset that resists change and innovation because "we've always done business this way" will ultimately prove fatal to that organization's future success and possibly even to its existence. Over the next 5 years at DSS we will take a careful and deliberate look at how we approach effective risk management by evaluating and refining our organization and

structure, our methodologies, and our ability to conduct in-depth analytics to ensure that we are providing optimal oversight, partnership, and educational services to our stakeholders.

Objective 1.2: Proactively analyze and plan for impacts of emerging law, policy, plans, and processes on DSS mission execution

Our agency functions as one component of the security community responsible for ensuring our Nation is protected and secure. To fulfill our mission, DSS is required to be responsive to change from a wide variety of sources, such as new law and policy being developed in the security arena by Congress and DoD or the impacts stemming from security breaches and events. National and DoD guidance has the potential to significantly impact and even shift what DSS does and the manner in which we do it; consequently, DSS will work proactively to analyze and inform developing guidance so that the agency is ready to respond in an effective and efficient manner once it is issued.

Objective 1.3: Support national and DoD initiatives to improve security programs, processes, and practices

Part of proactively mitigating risk is to support and influence the development of initiatives that will contribute to a more effective national security posture. DSS will actively pursue opportunities to provide subject matter expertise for the development of national and DoD initiatives that seek to provide better security risk management and mitigation programs that enable our industry and government partners to enhance security of our Nation's most valuable assets. This will fulfill the mission given in our charter; namely that DSS will support DoD efforts to improve security programs and processes.

Objective 1.4: Conduct contingency planning for potential new operations

Change has been a part of DSS' world since its inception in 1972. Today, however, change is taking place at a faster pace and in greater leaps than ever before. Over the next five years, in addition to responding to developments at the DoD and national levels, DSS will continue to develop our internal ability to anticipate possible future scenarios that could dramatically change either our mission or its execution. The proactive planning efforts that

result will reduce response time and enhance the agency's ability to rapidly recognize and adapt to those changes should they become reality.

Goal 2:	Enable government and industry stakeholders to proactively manage risk

As a security oversight and educational agency, at DSS we directly mitigate risk by refining our internal approaches and by proactively adjusting to a changing environment. Along with other security stakeholders — our cleared industry and government partners — we form the front line of defense that prevents adversaries from damaging our national security through espionage, theft, and insider threats. DSS mitigates risk by helping those stakeholders strengthen their defenses. We will do this by providing our partners with top quality and readily accessible education and training, in-depth and timely analysis, and comprehensive insights and best practices that help our partners improve their own risk management and mitigation processes.

Objective 2.1: Facilitate the availability of security education, training, and certification products and services

The constant state of change in how mission objectives are achieved in the 21st century global environment requires continual evolution and refinement of security practices and

procedures. DSS, through its functional community manager role for security education, training, and certification, is able to proactively address force readiness for security roles and responsibilities. We will do this by equipping DoD and industry personnel with timely and relevant security products and services available on demand.

Objective 2.2: Develop relevant and innovative content and services to support security awareness and information reporting

Resource constraints and the need for enhanced efficiencies within the security enterprise pose challenges to addressing ever changing security risks. Through strategic product and service design, DSS is equipped to expand delivery beyond traditional means. We will do this by developing new, or redesigning existing, security education and training products and services to enhance security awareness.

Objective 2.3: Provide timely, relevant, and accurate analysis to DSS, industry, and government decision makers

With the advent of globalization and big data accessibility, the aphorism "Knowledge is Power" applies perhaps more today than to any other time in history. Possessing a unique relationship with DoD, dozens of federal agencies, and more than 10,000 cleared contractors, DSS has the powerful ability to access and analyze broad streams of data that help provide an advantage when it comes to protecting our Nation's secrets. Between now and 2020, we will increase our support to national security by developing and providing our partners with significant trends, in-depth conclusions, and anticipatory practical responses based on analysis.

Objective 2.4: Foster a proactive, risk-focused culture among our stakeholders and partners

While technology is vital for a strong security program, the importance of process and procedure should not be underestimated. This is true even in today's cyber-predominant environment. The dangers of data exfiltration by physical or cyber theft are increased by the complex relationships connected to cleared industry today — insider threats, foreign interrelationships, and multiple sub-contractors, to name a few. DSS interactions with

cleared industry and government stakeholders provide the opportunity to share insights and recommendations on ways to reduce the risk of security breaches and to more rapidly respond should attacks occur.

As we proactively share with our stakeholders the scope of harm done by the loss of sensitive and classified information to our adversaries, we can positively influence their processes and procedures to minimize and mitigate the risks that could significantly impact our national security.

Objective 2.5: Expand delivery of security education, training, and certification products and services beyond the DoD

As the security environment within the U.S. Government grows in complexity, there is currently no shared approach for addressing the critical knowledge and competencies necessary to assure protection of national security. Across the U. S. Government enterprise, security education and training is disjointed, inconsistent, inefficient, and uneconomical.

DSS has a successful model for the development of a security professionalization program that can be expanded across the federal government. We will do this through partnership and development of common security skill standards and delivery of education, training, and certification designed to address federal security competencies.

Goal 3: Strengthen national security partnerships

As stated in the 2014 National Intelligence Strategy, partnerships "are fundamental to our national security." Cooperation and collaboration are key requirements for ensuring our Nation's security. With the increasing need for sharing information and the need to interact and work jointly with multiple security organizations, DSS seeks to formalize and expand the agency work already begun to establish, develop, and prioritize key relationships within the intelligence and security communities .

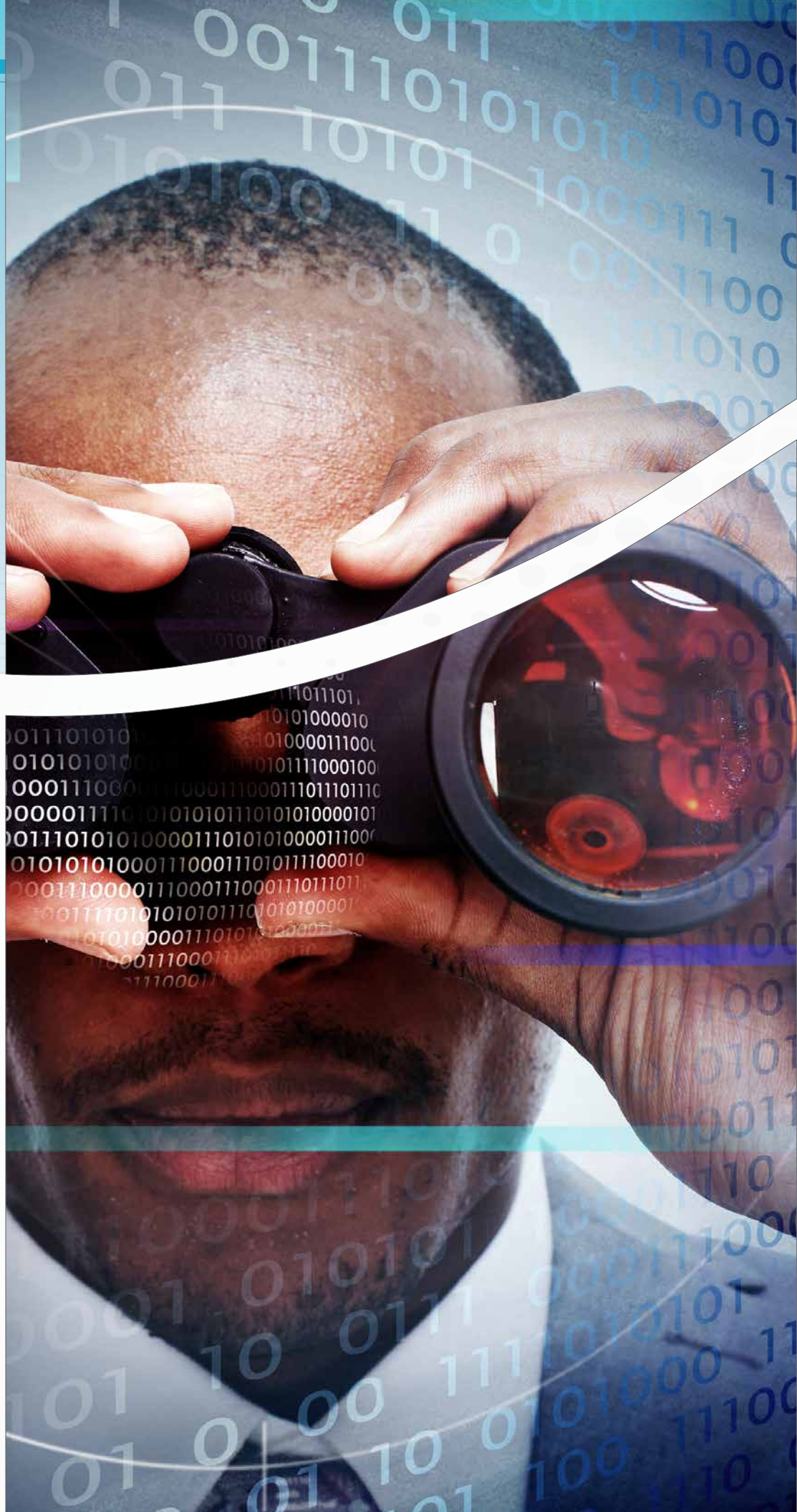
Encompassed by focused and intentional interaction, the contribution of DSS expertise to new security initiatives and increased information sharing within the security community, DSS will continue to build strong partnerships.

Objective 3.1: Execute a comprehensive strategic outreach program

The first step in increasing partnerships is to create a formal program that will frame DSS outreach efforts. DSS will build a partnership program by formally identifying, prioritizing, and engaging key stakeholders; establishing appropriate levels of interaction and involvement; and by consistently evaluating both the risks and the benefits of our outreach efforts. We will also continue to partner with cleared industry and government stakeholders to develop proactive rather than reactive security solutions and to build strong, comprehensive relationships that encourage transparency and the sharing of information.

Objective 3.2: Grow existing and establish new partnerships

Within our outreach framework, DSS will intentionally reach out to other security agencies and organizations to build and strengthen valuable partnerships that will advance common goals and provide mutual support in the fulfillment of our individual roles and responsibilities for protecting the Nation. These efforts will result in greater familiarity with our partners' roles and missions, increased liaison and collaboration, and a broader understanding within the DSS workforce of potential gaps and similarities among the organizations that comprise the national security community. As a result, formal and informal ties will be developed and national security will be enhanced.



Objective 3.3: Support DoD and the U.S. Government in proactively shaping emerging security law and policy

Looking from our unique vantage point between government and industry, DSS has the ability to see firsthand the real impacts that law and policy coming from government and the DoD have on cleared industry. We also are able to rapidly identify areas where policy gaps create unnecessary security risks or uncertainty in industry practice. Where appropriate, as potential laws or policies are discussed and developed, DSS will provide wholehearted support and execution of our charter by lending our broad experience and expertise on industrial security to those responsible for the development of both law and policy.

Objective 3.4: Establish and better leverage existing collaboration networks and processes to manage/share information with stakeholders

Constructive partnerships can provide significant value to the agencies involved by facilitating the sharing of data through means such as the exchange of operational information, capabilities, requirements, best practices, lessons learned, and emerging trends, threats, and opportunities. However, for a variety of reasons, information that would provide a clearer situational picture and allow for better action and response by the security community is not always shared in a timely manner. As part of strengthening our national security partnerships, we will strive to support development of networks and processes that improve communication and the sharing of information and that enhance the common operating picture for DSS and our partners.

Goal 4: Empower a mission-driven workforce responsive to the changing environment

The most valuable resource available to our organization is our people; this is reflected in our motto: "people first, mission always." For DSS to succeed we need a workforce that is flexible, reliable, innovative, and dependable. By ensuring that our workforce is provided the opportunity to excel through training, mentorship, and increased responsibility, we can be assured that through their technical competence we are able to tackle our difficult mission in an ever-changing environment. By empowering our workforce, we enhance the

agency's ability to address issues we and the cleared industry face on a daily basis. We must systematically provide the resources, programs, and tools that allow DSS to thrive. Our workforce must be analytic and critical thinkers in an era of diminishing resources. We strive to provide opportunities for further skill development in order to improve upon our weaknesses and continuously improve our workforce.

Objective 4.1: Strengthen and sustain a diverse, technically competent, and professional workforce

Diversity is strength and we must maintain diversity infused with technically competent professionals. We have expertise, competence, and dedication to the DSS mission and we must utilize the differences in our backgrounds, cultures, and ideas and continue to build on our strengths and improve upon our weaknesses. By establishing a culture of continuous improvement, we can build a diverse and multi-skilled workforce embedded with appropriate redundancies, ensuring that DSS is always ready to accomplish its mission.

Objective 4.2: Grow leaders to meet the challenges of an evolving security environment

At DSS, all employees are leaders that inspire and motivate others. DSS employees lead by setting positive examples through their daily actions. However, to move the agency

forward and accomplish its mission, DSS must hone and shape its leaders by providing structured leadership development and associated resources and learning opportunities. By establishing a strong foundation and providing an environment where our current and future leaders can offer purpose, direction, and motivation, DSS can confidently lead cleared industry and our agency partners into the future.

Objective 4.3: Enhance recruitment, development, and retention strategies that foster a culture of collaboration and teamwork

The DSS workforce is the agency's most important asset. It is important to build a workforce that honors the agency values, embraces the mission, and strives for excellence. To do this we must find the best possible recruits that will not just fit into the DSS family but will make it better. We will ensure that our hiring practices are not only right but also efficient and will make the process easier for all involved.

We must retain our talented workforce by providing opportunities for diverse experiences and recognition and appreciation for accomplishments. Through these efforts we can help build and nurture a positive work culture supported by an experienced and motivated workforce that continually collaborates and has the flexibility to get the job done.

Goal 5: Provide enterprise solutions to improve operations and performance management

In today's uncertain world, organizations are continually encouraged to do more with fewer resources. This challenge is driven by the need for strategy and efficiency. With a sound strategy, organizations can move forward with a common and actionable purpose. Striving for optimal efficiency, organizations must lay the groundwork for strategic management of all their existing resources.

Ensuring integration and consistency through all DSS policies and processes across the organization and providing employees with the proper tools to complete their jobs supports the growth of efficiency and compliance with standards. By providing an organized, strategic, and supportive base, DSS can successfully work towards accomplishing its mission.

Objective 5.1: Establish and implement a sustainable strategic management framework

It is not enough for an agency to successfully achieve their mission with simply a strategic plan. It is essential to synchronize all strategic functions and effectively integrate these activities. The DSS Strategic Management Framework supports the effective and efficient implementation of the agency's mission while providing transparency throughout the entire organization.

Consisting of three overarching components — the DSS Strategic Plan, strategic functions, and performance evaluation and reporting — the framework will enable DSS to establish strategy; make informed decisions; and allocate and prioritize resources and strategic and operational activities.

Objective 5.2: Establish requirements and framework for defining and managing knowledge

Having served the Nation for decades, DSS has amassed a diverse base of knowledge supported by the expertise of the past and current workforce, as well as by lessons learned and internal reports, studies, and a number of other resources. The challenge comes in ensuring that this valuable information is readily available for analysis and decision-making and accessible to those who need it. Establishing a cohesive knowledge management

framework will help enable DSS to successfully utilize and apply the extensive resources that have grown within the agency.

Objective 5.3: Define, develop, and deliver tools and capabilities to enhance agency operations

The strategic environment, with its persistent threats, challenges, and budget restrictions, along with the complexity of the DSS mission, requires that the agency regularly modernize its business solutions and processes in order to maximize efficiency and reduce waste. Ensuring that the best tools are in place supports DSS in performing its essential functions, supporting stakeholders, and supporting national security.

Objective 5.4: Improve and document policies and processes that govern internal operations to optimize mission execution, ensure consistency, and clarify intent across the enterprise

While a policy documents protocol and serves as a guide for actions and decisions, processes provide instructions for completing certain actions. To align with the DSS Strategic Management Framework, DSS should have formal and documented policies and processes that provide a common operating base and help guide employees in their actions and in completing their duties in support of the organization. This guidance provides accountability and ensures consistency and integration among all key activities within the agency. Periodic reviews will verify that policies and processes are operating effectively in the ever-changing environment. Additionally, new policies and processes should be reviewed and documented as the need for additional guidance is identified.

Objective 5.5: Evaluate operational and support requirements, services, and products to identify efficiencies and cost savings

In today's resource constrained environment, organizations are urged to do more with less. In addressing this challenge, we will look for ways to centralize information and data, prioritize efforts, streamline processes, and reduce redundancies. In becoming more efficient, DSS will be prepared to consistently complete its mission while handling resource challenges and opportunities that emerge in the future.

DSS Strategic Plan 2020

Strategy Map

GOAL 1

Strengthen capabilities to continually identify, evaluate, and mitigate risk to the DoD and national industrial security base

1.1	Assess, analyze, and continuously enhance DSS' approaches to risk management
1.2	Proactively analyze and plan for impacts of emerging law, policy, plans, and processes on DSS mission execution
1.3	Support National and Department of Defense initiatives to improve security programs, processes and practices
1.4	Conduct contingency planning for potential new operations

GOAL 2

Enable government and industry stakeholders to proactively manage risk

2.1	Facilitate the availability of security education, training and certification products and services
2.2	Develop relevant and innovative content and services to support security awareness and information reporting
2.3	Provide timely, relevant, and accurate analysis to DSS, Industry, and Government decision makers
2.4	Foster a proactive, risk-focused culture among our stakeholders and partners
2.5	Expand delivery of security education, training and certification products and services beyond the DoD

GOAL 3

Strengthen national security partnerships

3.1	Execute a comprehensive strategic outreach program
3.2	Grow existing and establish new partnerships
3.3	Support DoD and the U.S. Government in proactively shaping emerging security law and policy
3.4	Establish and better leverage existing collaboration networks and processes to manage/share information with stakeholders

Vision

Through partnership and innovation, safeguard our Nation's interests as the premier provider of industrial security risk management and security professional development services.

Mission

The Defense Security Service (DSS) strengthens national security at home and abroad through our security oversight and education operations. DSS oversees the protection of U.S. and foreign classified information and technologies in the hands of cleared industry under the National Industrial Security Program by providing professional risk management services. As Functional Manager for the Department of Defense (DoD), DSS provides security education, training, certification, and professional development for the DoD and for other U.S. Government personnel, contractor employees and representatives of foreign governments.

GOAL 4

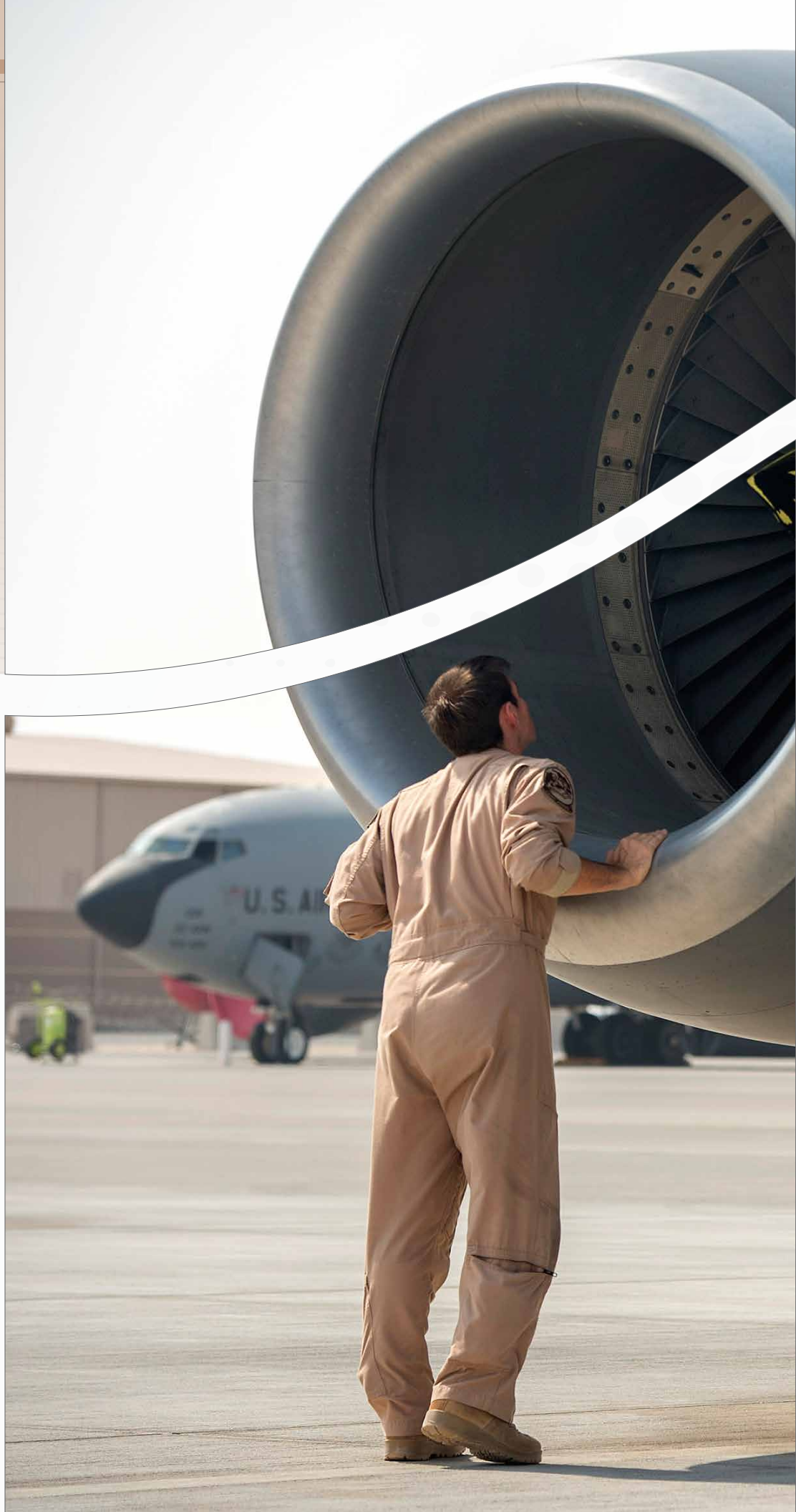
Empower a mission-driven workforce responsive to the changing environment

4.1	Strengthen and sustain a diverse, technically competent, and professional workforce
4.2	Grow leaders to meet the challenges of an evolving security environment
4.3	Enhance recruitment, development and retention strategies that foster a culture of collaboration and teamwork

GOAL 5

Provide enterprise solutions to improve operations and performance management

5.1	Establish and implement a sustainable strategic management framework
5.2	Establish requirements and framework for defining and managing knowledge — [collection, storage, analysis and sharing of information]
5.3	Define, develop and deliver tools and capabilities to enhance agency operations
5.4	Improve and document policies and processes that govern internal operations to optimize mission execution, ensure consistency, and clarify intent across the enterprise
5.5	Evaluate operational and support requirements, services, and products to identify efficiencies and cost savings



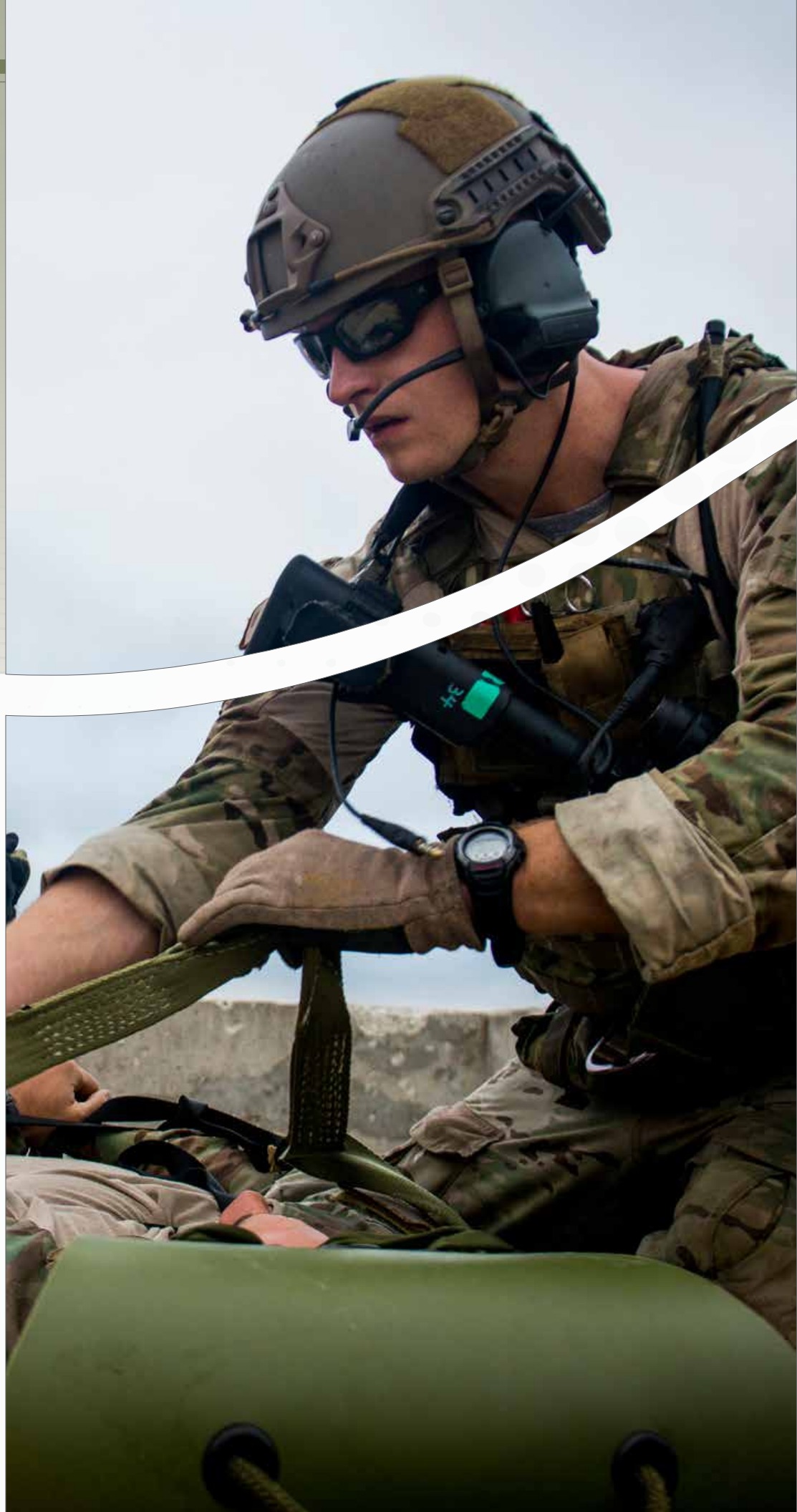
Strategic Plan Management

Strategic Plan Development

Every four years, or as directed by DSS leadership, DSS will develop a new strategic plan. This deliberative process will include an in-depth review of the organization's mission, vision, and values, as well as a study of organizational goals, objectives, and performance goals looking from the present out to the next five to seven years.

Strategic Plan Revision

The DSS Strategic Plan will be reviewed annually. The annual review will evaluate the current strategic objectives and performance goals and will solicit input from DSS directorates, senior leaders, DoD guidance, law and/or policy changes, and changes to the current or future strategic operating environment.



Implementation Plan

Director's Strategic Planning Guidance

The DSS Director's Strategic Planning Guidance (SPG) is published on an annual basis. This document establishes selected strategic plan goals as agency priority goals for the coming year. The SPG is synchronized and in agreement with the annual DSS Program Objective Memorandum (POM) submission, and is included as part of the DSS Annual Implementation Plan.

DSS Annual Implementation Plan

The DSS Annual Implementation Plan includes the annual SPG and establishes how DSS will work toward accomplishing the goals, objectives, and performance goals of the DSS Strategic Plan. While performance goals may be revised over the life of the Strategic Plan, at the time of the initial DSS Strategic Plan 2020 publication DSS has identified 115 specific performance goals that, when accomplished, will fulfill the Plan's strategic goals and objectives.

The Implementation Plan will identify Offices of Primary and Coordinating Responsibility (OPR/OCR) for each performance goal, OPR/OCR roles and responsibilities, and methods for reporting and oversight. The Annual DSS Implementation Plan establishes the mechanism for tracking the successful completion of the DSS Strategic Plan by providing visibility to the governance councils on the qualitative and quantitative metrics and measures that demonstrate progress, especially for the agency priority goals identified in the SPG.

Upon its release, DSS directorates will incorporate the Implementation Plan into individual employee plans for the coming fiscal year. DSS Annual Implementation Plan progress will be reviewed on a regular basis during the established DSS governance cycle.

Conclusion

As stated in the foreword to the 2014 National Intelligence Strategy, the threats we face today are the most diverse our nation has experienced in the last 50 years. Our response, embodied in this holistic and dynamic plan, helps to ensure that those threats do not damage the security of our nation.

This plan energizes the entire DSS strategic management framework and provides the momentum for successful mission accomplishment into the future. Agency decisions, priorities, and resources will be evaluated by how they support the goals and objectives of this plan.

As our leaders and managers work toward the completion of those goals and objectives in their functional areas, and as every member of our workforce does their part for successful implementation, together we will continue to effectively fulfill our unique and vital role in safeguarding our nation's interests.

Acronyms

CDSE	Center for Development of Security Excellence
CI	Counterintelligence
DISP	Defense Industrial Security Program
DoD	Department of Defense
DoDD	Department of Defense Directive
DSS	Defense Security Service
EO	Executive Order
IO	Industrial Security Field Operations
IP	Industrial Security Integration and Application
KM	Knowledge Management
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
OCR	Office of Coordinating Responsibility
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPR	Office of Primary Responsibility
POM	Program Objective Memorandum
SPG	Strategic Planning Guidance
USDI	Under Secretary of Defense for Intelligence

Defense Security Service

DSS Strategic Plan 2020