STRATEGIC PLAN 2022-2027

Defense Counterintelligence and Security Agency

May 2022

Intentionally left blank

MESSAGE FROM THE DIRECTOR

I am pleased to present the first Defense Counterintelligence and Security Agency (DCSA) Strategic Plan, covering the period 2022 - 2027. When DCSA formed at the end of 2019, we merged several distinct organizations to better accomplish the nation's security missions. This integration is foundational to building the best possible security enterprise to defend the United States from extant and future adversaries attempting to gain a national security advantage through our workforce, technologies, and supply chain.

Since DCSA's founding, we have focused on combining legacy organizations by improving performance and operating as a single agency. Having achieved this initial objective, this strategic plan takes the next step—providing a roadmap for DCSA to follow during the next five years as we seek to optimize our mission performance.

This strategic plan provides a framework for how DCSA will answer new security challenges facing industry, the federal workforce, and the nation's critical information, technologies, and supply chain. The plan lays out the goals and objectives we must accomplish to safeguard the trustworthiness of America's workforce and lead the conversation regarding necessary changes to improve security of the national industrial base.

The plan will guide our steps as DCSA seeks to optimally leverage the resources, people, and capabilities that will enable the Agency to ensure the security of our nation, technologies, and information. The plan aligns our activities with others within the Department of Defense (DOD) and the Federal Government. Further, it will serve as the basis for budgetary prioritization, requirements definition, and resource management.

Upon becoming DCSA Director, I was charged not only with integrating and maturing the new agency, but also with transforming its capabilities and processes. Even without that mandate, which is understandable for any new organization of DCSA's size, transformation is absolutely necessary today to meet the evolving threat landscape and the return of great power competition. This strategic plan represents a commitment to that transformation journey and provides a framework to guide DCSA leaders in developing roadmaps that will take us there.

I am committed to successfully implementing this strategic plan and continuing DCSA's world-class mission execution. In that regard, we cannot be passive. Together, we are America's Gatekeeper, and our nation's security depends not merely on consistent performance but on consistently improved performance as envisioned in this strategic plan. Please read it, embrace it, and work to implement it as if our national security depended on it. It does.

Sincerely,

William K. Lietzau, Director, DCSA

"Embrace this strategy as if our national security depended on it. Because it does."

Intentionally left blank

CONTENTS

1 Introduction
5 Industrial Security
6 Personnel Security
7 Counterintelligence & Insider Threat
8 Security Training
9 Talent
10 Unity of Effort
11 Operational Effectiveness
12 Digital Ecosystem
13 Resourcing Processes
14 Strategy Implementation and Management
15 Conclusion
16 Acronyms
17 References

Intentionally left blank

INTRODUCTION

As America's Gatekeeper, DCSA ensures the security of the national industrial base (e.g., cleared contractor base and priority supply chains) and the federal employee workforce. America's rivals hurt the nation economically and militarily by stealing proprietary and classified information, subverting our capabilities, sowing disinformation, and undermining the trust of our employees and industry partners. Our adversaries are persistent and exploit all opportunities. DCSA was created to meet these threats.

The signing of Executive Order 13869 in April 2019 established the mandate to create DCSA. Since then, the Agency has grown substantially in both size and complexity.

1

On October 1, 2019, the Defense Security Service (DSS), the National Background Investigations Bureau (NBIB), and the DOD Consolidated Adjudications Facility (CAF) merged to form DCSA.[1]

2

In October 2020, legacy information technology systems were realigned to DCSA from the Office of Personnel Management (OPM), the Defense Manpower Data Center (DMDC), and Defense Information Systems Agency's (DISA) National Background Investigation Services (NBIS) program office. This second wave of transfers included integrating the Personnel Vetting Transformation Office and supporting personnel from DISA's Joint Service Provider and DMDC's Defense Human Resources Activity.

3

In October 2021, the National Center for Credibility Assessment (NCCA) transferred from the Defense Intelligence Agency (DIA) to DCSA's Security Training Directorate, and discussion began regarding other security-related mission transfers.

Combining these organizations united the Federal Government's essential security functions of personnel security, industrial security, security training, and counterintelligence and insider threat support in one agency.

Today, DCSA encompasses a workforce of more than 12,000 government employees and contractor personnel operating from more than 160 regional and field offices throughout the United States. This broad geographical dispersion keeps DCSA's workforce on the front lines of the effort to protect the trustworthiness of the defense industrial base (DIB) and the federal workforce.

[1] Executive Order 13869, April 2019

DCSA is directly affected by many developments that change how the nation defends its way of life, including new policies, new technologies, and an ever-changing threat landscape.

New security policies

- **Personnel Security:** The Federal Government's rollout of Trusted Workforce (TW) 2.0, an initiative that seeks to manage risk through an end-to-end personnel vetting process, is a massive transformation for vetting individuals.
- **Industrial Security:** A "whole-of-government" approach to industrial security does not exist to the same extent that it does for personnel security. But new initiatives such as Section 847 of the National Defense Authorization Act for Fiscal Year 2020, "Mitigating Risks Related to Foreign Ownership, Control, or Influence (FOCI) of DOD Contractors or Subcontractors," highlight the growing interest in expanding entity vetting services to ensure the integrity of the supply chains supporting the DOD and other federal priority programs.

Technological advancements

- The rapid pace of technological advancement expands the scope of the security mission as new technologies become critical and need to be protected from our adversaries. Protecting these technologies becomes more complex as the need to secure systems outside the classified environment grows. For DCSA, technology is also an enabler to meet the growing vetting mission's need to analyze and share massive volumes of data.

Changing threat environment

- The threat environment has shifted from one yielding a predominant focus on counterterrorism activity to one requiring a renewed focus on great power competition. In this environment, U.S. industrial base supply chains and the federal workforce are primary targets to gain an advantage. Our adversaries actively target sensitive data, critical and emerging technologies, and intellectual property with sophisticated cyber-enabled espionage, human intelligence assets, and emerging technologies. At the same time, insider threats are also growing as the workforce is targeted by strategic actors, terrorists, and domestic extremists.

These conditions put DCSA at the forefront of great power competition, requiring an increased focus on the industrial security mission and countering threats posed by our strategic adversaries as well as implementation of personnel security changes appropriately designed to meet today's threat. DCSA is meeting these challenges by undertaking an enterprise-wide transformation to unify efforts across missions to better identify and mitigate threats. DCSA's unique mission and role in the Federal Government makes the Agency an essential resource to receive, collate, and disseminate information across multiple customers, partners, and stakeholders.

DCSA will not succeed in this mission by acting alone. We will participate in and, where appropriate, lead the discussion with DOD, the broader Federal Government, and the DIB. The ability to partner with internal and external stakeholders aligns with the 2021 Defense Security Enterprise Strategy, which states, "[e]nterprise stakeholders and partners must work together to reduce misalignment and wasted resources that hinder progress toward elevating security." DCSA will "manage security programs, conduct security operations, and integrate the security community to increase its effectiveness." [2]

[2] Defense Security Enterprise Strategy, July 2021

Since 2019, DCSA has successfully improved its execution of statutory missions even as it undertook the complex integration of legacy organizations under a new enterprise-wide operating model. With that integration now complete, DCSA is focused on executing its five-year strategic plan and meeting the challenges presented by the evolving threat environment. DCSA will focus on unifying efforts across missions and becoming a fully integrated, operationally focused agency supporting the National Defense and Intelligence Strategies.

DCSA unifies its efforts through its Mission, Vision, and Values. The Mission shares the Agency's purpose with employees, customers, and partners. The Vision sets the goal for the future. DCSA's Values guide the Agency on how it does its work.

Mission

Through vetting, industry engagement, education, and counterintelligence and insider threat support, secure the trustworthiness of the United States Government's workforce, the integrity of its cleared contractor support, and the uncompromised nature of its technologies, services, and supply chains.

Vision

Optimize our performance as the preeminent security organization to protect our nation's critical assets through enterprise risk management, continuous innovation, and excellence in mission performance and customer service.

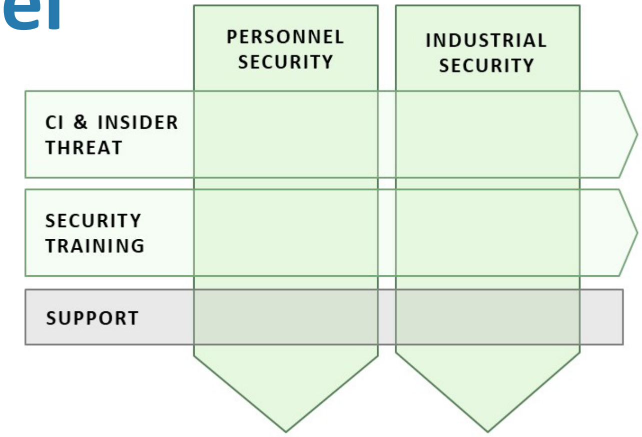
Values

COMMITTED TO MISSION
PASSIONATE ABOUT SERVICE
UNWAVERING IN INTEGRITY
DRIVEN TO INNOVATE
INVESTED IN PEOPLE

Vetting Operating Model

Shortly after its creation in 2019, DCSA began work on a new operating model to define how the Agency's core missions and support functions should come together to deliver mission performance. The operating model depicts four mission areas: two primary security missions, Personnel Security and Industrial Security, and two enabling missions, Counterintelligence and Insider Threat and Security Training.

Support functions provide a foundation for delivery of our growing and dynamic missions. And with all our mission areas working together, the entire lifecycle of Vetting Services manages risk and works directly with our customers to deliver a trusted workforce and secure the nation's critical data.



Operating Model, *key*

🟩 Mission Area

Arrow denotes delivery of services to customers and internally

⬜ Support Area

Includes enabling and mission support functions

The operating model is grounded in a set of **design principles** that shift the Agency from:

- Manual processes → Automated processes
- Compliance-based operations → Risk-based operations
- Siloed organizations → Integrated organization
- Ad hoc services → Standardized services
- Resource-intensive methods → Requirements-driven methods
- Agency-centric focus → Customer-centric focus

The operating model describes how the Agency will optimize its mission performance. The strategic plan describes the desired outcomes toward which DCSA will focus efforts, along with the specific actions we will take to achieve these outcomes. Starting in fiscal year 2022, investment decisions and resource allocations will be linked with validated requirements and aligned with the operating model and the strategic plan.

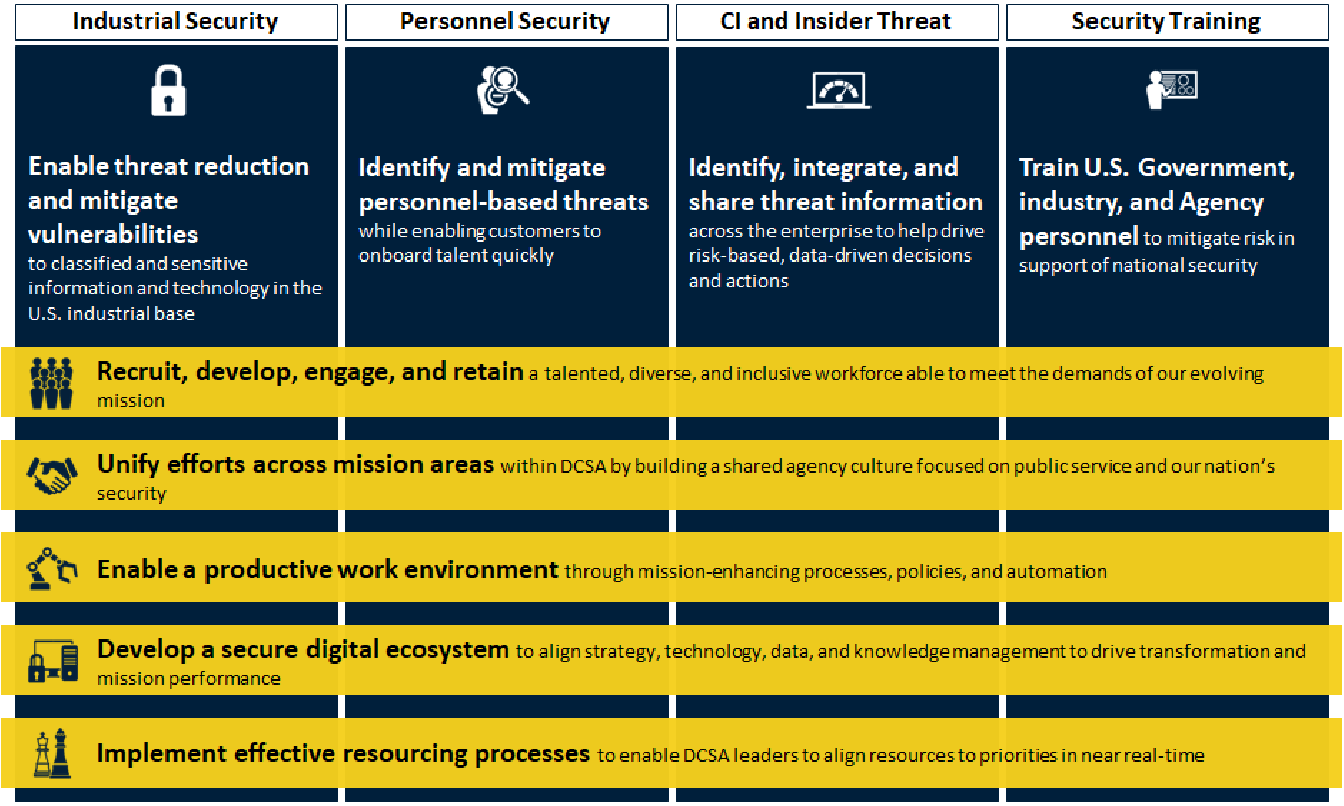
DCSA has identified nine goals that collectively form the Agency's strategy to achieve its vision and become the nation's preeminent security organization. Meeting these goals will transform how DCSA reduces risk across the defense supply chain and the trusted workforce. The goals are divided into two categories: mission goals (listed in the columns below) and enterprise goals (listed in the rows below). All nine goals are necessary and mutually supporting to deliver our mission to the nation.

MISSION GOALS

Advancing mission performance through unity of effort, partnership, and customer experience

ENTERPRISE GOALS

Empowering people and transforming enterprise capabilities to support an expanding Agency and mission



Industrial Security

Enable threat reduction and mitigate vulnerabilities to classified and sensitive information and technology in the U.S. industrial base

Personnel Security

Identify and mitigate personnel-based threats while enabling customers to onboard talent quickly

CI and Insider Threat

Identify, integrate, and share threat information across the enterprise to help drive risk-based, data-driven decisions and actions

Security Training

Train U.S. Government, industry, and Agency personnel to mitigate risk in support of national security

Recruit, develop, engage, and retain a talented, diverse, and inclusive workforce able to meet the demands of our evolving mission

Unify efforts across mission areas within DCSA by building a shared agency culture focused on public service and our nation's security

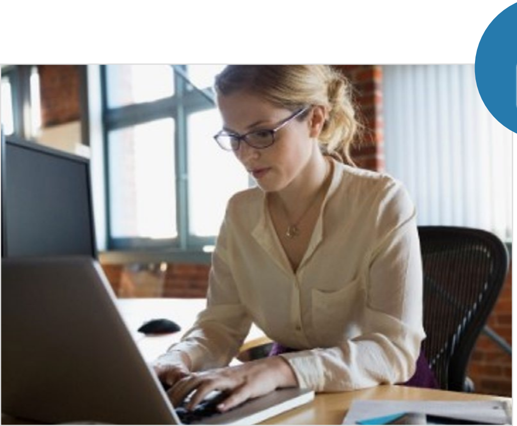
Enable a productive work environment through mission-enhancing processes, policies, and automation

Develop a secure digital ecosystem to align strategy, technology, data, and knowledge management to drive transformation and mission performance

Implement effective resourcing processes to enable DCSA leaders to align resources to priorities in near real-time

Each of the nine strategic goals comprises three to five mutually reinforcing objectives, which, when executed successfully, will result in the attainment of the goal.

To operationalize the strategy, each strategic goal will be assigned an enterprise goal champion from DCSA's senior leadership team. The champion will be responsible for ensuring DCSA successfully accomplishes each goal. Supporting objectives will be assigned to DCSA leaders, who will have responsibility for executing the program of work necessary to achieve each objective.



Mission Goal

Enable threat reduction and mitigate vulnerabilities to classified and sensitive information and technology in the U.S. industrial base. Executive Order 13869 charges DCSA with securing "classified and sensitive information and technology in the U.S. industrial base against attack and compromise."[3] The Industrial Security mission ensures that the organizations and contractor workforce within the National Industrial Security Program (NISP) can be trusted with sensitive and classified information.

DCSA mitigates risks in the cleared contractor base by various processes including:

- Vetting commercial entities and issuing contractor facility clearances
- Establishing agreements and legal instruments to address FOCI
- Conducting security and cyber oversight, to include the introduction of new procedures and maturation of risk-based approaches

Today's dynamic security environment demands that DCSA expand its role into new mission areas to yield a more holistic regime for protecting the nation's critical technology and services. One future expansion to support broader supply chain integrity and resilience is the implementation of the requirements outlined in Section 847 of the National Defense Authorization Act for Fiscal Year 2020 regarding beneficial ownership. This new law requires expansion of existing NISP FOCI risk analysis for a significant number of companies that are not under NISP oversight but are integral to the DOD supply chain. NISP policy also requires an expansion of DCSA's mission to include establishing a controlled unclassified information (CUI) program management office and could expand further to include other security missions and services such as accreditation of sensitive compartmented information facilities, operational security, information security, and physical security of DOD installations.

DCSA will work with the Defense Security Enterprise and the appropriate policy offices within the Office of the Secretary of Defense to define, plan for, and implement the expanding mission requirements. To gain efficiencies in its core missions while implementing the emerging ones, DCSA will collaborate with stakeholders to invest in identifying, developing, and deploying new technology and information systems necessary to understand and respond to threats and risks posed by adversaries. DCSA will also ensure that the data is available to improve information sharing with industry (from small businesses and startups to large contractors with multiple secure facilities), government customers, and other appropriate partners to facilitate understanding of the risk to their organizations and programs and to take any necessary mitigating actions. DCSA will also use its access to the DIB to contribute to a broader U.S. Government (USG) understanding of risk to its supply chain and industrial base.

Objectives

1

Identify threats and vulnerabilities and understand risk across the NISP and the appropriate DIB elements to protect critical warfighting technologies and other capabilities.

2

Mitigate risk through collaboration, security and cyber oversight activity, and direct guidance.

3

Develop a digitally-enabled common operating picture of risk across the defense supply chain and share information with government customers and industry partners.

[3] Executive Order 13869, April 2019

PERSONNEL SECURITY

Mission Goal

Identify and mitigate personnel-based threats while enabling customers to onboard talent quickly. With the TW 2.0 initiative, the Federal Government is transforming how it vets individuals for the trusted workforce, with the goal of driving integration, transparency, efficiency, and effectiveness in all aspects of personnel vetting. To meet the TW 2.0 vision, DCSA will implement the TW policy framework, including building and operating the Federal Government's end-to-end system for vetting services (the National Background Investigation Services or NBIS). The system and related processes will fulfill trusted workforce requirements including initiation and assignment of clearance cases, investigations, adjudications, continuous vetting operations, case management, and data repository needs. It will cover all five personnel vetting scenarios including: initial vetting, continuous vetting, transfer of trust (reciprocity), upgrade in trust, and re-establishment of trust.

NBIS will deliver enterprise capabilities to manage personnel vetting processes from initial application through final vetting. NBIS will replace a set of legacy applications and a series of highly manual steps in the personnel vetting value chain. In addition to technical delivery, DCSA will place a significant focus on adoption among internal and external users and stakeholders by ensuring the program is fit for its purpose and optimized for user requirements and experience. DCSA's emphasis on delivering NBIS is driven by a commitment to improving timeliness, elevating the customer experience, and improving the quality of vetting services.

Full implementation of TW 2.0 includes developing and implementing new processes that leverage NBIS and related capabilities to increase the overall security of the trusted workforce and will enable all four objectives.

Objectives

1

Implement the Trusted Workforce framework and deliver high-quality, timely products across all personnel vetting scenarios.

2

Identify and mitigate threats and vulnerabilities among USG (including non-DOD and DCSA internal) and partner personnel.

3

Improve customer experience, including enhanced process transparency, increased information sharing, and streamlined product delivery.

4

Develop and deploy NBIS to necessary government customers and stakeholders to facilitate TW 2.0 initiatives.

COUNTERINTELLIGENCE & INSIDER THREAT

Mission Goal

Identify, integrate, and share threat information across the enterprise to help drive risk-based, data-driven decisions and actions. The DCSA Counterintelligence and Insider Threat Directorate identifies foreign intelligence entities and threat actors who intend to disrupt the Department's critical technology and sensitive information by targeting cleared contractors, cleared personnel, and DCSA. This directorate will expand to better deny and disrupt strategic competitors and trusted insiders' malicious intent through analysis of information and intelligence, the management and oversight of the insider threat enterprise, and execution of CI functional services, including through expansion into the personnel security investigation support arena.

DCSA will collaborate with mission partners, cleared industry, and other government agencies to detect, deter, assess, disrupt, and mitigate CI, cyber, and insider threats. DCSA will invest in personnel, focus resources, enhance business practices, and leverage technological innovation to share CI reporting, threat indicators, and emerging trends to accelerate mitigating actions.

Threats and vulnerabilities in the cyber domain have emerged as critical vectors that adversaries use to target sensitive U.S. information. DCSA has a strong cyber threat identification foundation and will build upon its robust suite of cyber threat awareness capabilities. The Agency will continue to invest in innovative cyber technology, enterprise tools, and technical professionals to counter the nation's strategic competitors and their proxies' malicious cyber activity.

DCSA will increase both the depth and the breadth of our partnerships. Through continuous engagement with the Intelligence Community, law enforcement organizations, and the military departments, DCSA will expand foreign intelligence entity and insider threat actor awareness through information sharing.

DCSA will use an enterprise approach for security risk management, aligning its capabilities with other DOD and government agencies. By integrating mission sets, DCSA will better collect threat and vulnerability information, identify, analyze, and prioritize risk, and disseminate analytical results. This will create a risk-informed decision-making process in near real-time, accessible by stakeholders throughout the government and cleared industry.

Objectives

1

Identify, assess, and disrupt threats to cleared industry, cleared personnel, DOD, and DCSA through the application of Counterintelligence, Cyber, and enterprise insider threat management activities.

2

Facilitate USG responses to adversary action and insider threats by sharing threat indicators and enabling responsive measures from other agencies and services.

3

Develop cyber capabilities and processes that illuminate threats, enhance awareness, and enable customer response.

4

Develop and operationalize an enterprise security risk management methodology across government and industry stakeholders.

Mission Goal

Train U.S. Government, industry, and Agency personnel to mitigate risk in support of national security. The DCSA Security Training Directorate encompasses the National Center for Credibility Assessment (NCCA) and the Center for Development of Security Excellence (CDSE). The Security Training Directorate develops the capability of security professionals across the federal enterprise to equip them to address tomorrow’s challenges. DCSA’s training efforts protect the nation by providing security training, education, certification, and research. This includes having the operational agility to rapidly respond to the needs of the defense enterprise to develop and deliver curricula that build tangible capabilities and close gaps in abilities as they are encountered. These activities span a broad spectrum of security and counterintelligence disciplines, including credibility assessment, industrial security, personnel security, physical security, information security, and insider threat.

DCSA will leverage technology to improve the substance and accessibility of its materials to ensure customers receive rapid and timely delivery of critical information precisely where and when it is needed. A vital component of this will be using technology to provide innovative training techniques and expand our partnerships into non-traditional areas (e.g., support allied nations and other government agencies) to efficiently mitigate security risks wherever they may be found. The Security Training Directorate provides products and services based on established and recognized security standards that promote consistent application of security practices. The Security Training Directorate strives to expand partnerships to extend the access and usage of these existing products and services to widen the landscape of those prepared to protect national security assets within and beyond DOD, where applicable.

In addition to providing comprehensive security training, DCSA will continue to support the nation’s security through federal credibility assessment capabilities, including conducting clinical and field research, and developing, testing, and evaluating credibility assessment technologies and methods. DCSA will also ensure the continued readiness of federal polygraph programs by providing technical support and assistance through required oversight inspections. These inspections ensure polygraph program readiness is maintained and examinations are conducted ethically in accordance with federal statutes and policies.

Objectives

1

Advance and expand products and services to meet the evolving needs of mission partners.

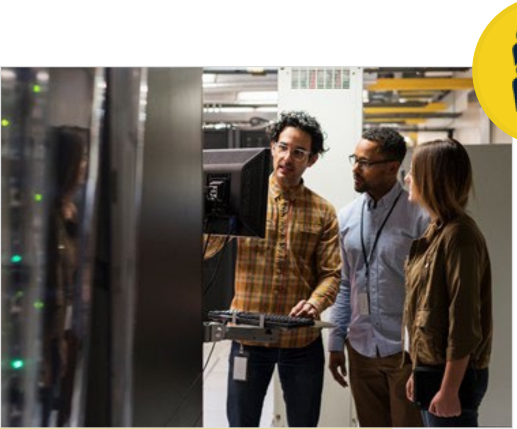
2

Leverage technology to modernize the customer experience and rapidly deliver products.

3

Partner to expand our customer base to promote the consistent application of security standards.

Enterprise Goal



Recruit, develop, engage, and retain a talented, diverse, and inclusive workforce able to meet the demands of our evolving mission. DCSA's unique mission places a priority on attracting, onboarding, retaining, and developing the Agency's future and current workforce. This necessity flows to all DCSA mission areas. To meet these requirements, DCSA will build the workforce through recruiting diverse, qualified talent, and through workforce development.

This will include modernizing and improving processes, for example, by:

- Implementing a recruitment strategy to enable the Agency to attract and retain diverse, qualified talent in an effective and efficient manner to support the Agency's mission.
- Developing and implementing a DCSA Strategic Workforce Plan to identify and ensure the right mix of skills and competencies needed to accomplish the mission.
- Leveraging technology and process improvements to streamline human capital operations.
- Incorporating new technologies and methodologies to support data-driven, strategic workforce planning and decision-making processes across the Agency.
- Cultivating collaborative leaders who can help their teams contribute to the goal of a unified organization and mission success.

Objectives

1

Support our future and current workforce through best-in-government applicant and employee experience, benefits, training programs, and career management services.

2

Develop and refine strategic workforce plans to adapt to dynamic mission requirements and emerging innovative capabilities.

3

Grow DCSA capabilities with digital platforms to accelerate transactions, inform data-driven decisions, and enable resource planning.

4

Cultivate a skilled, multidisciplinary workforce and capable, collaborative leaders.

UNITY OF EFFORT

Enterprise Goal

Unify efforts across missions within DCSA by building a shared agency culture focused on public service and our nation's security. DCSA must transition from a collection of discrete missions operating in silos to an integrated security mission, working collectively as a single agency. Achieving this goal will require a mindset shift toward unity of effort in everything DCSA does.

This cultural shift will be successful if conditions are set to enable the missions to work more closely together, for example, by:

- Adopting an “enterprise mindset” that asks DCSA employees to put the good of the Agency’s mission before their specific mission area (e.g., resource reallocation).
- Providing clear guidance on information sharing parameters across the Agency.
- Establishing and maturing DCSA’s new regional structure and headquarters to provide integrated operational leadership in the field.
- Building strong partnerships and standardizing DCSA’s customer experience capabilities through the implementation of an enterprise customer experience strategy.

DCSA will raise awareness of its mission impact among customers, industry partners, and stakeholders through these partnerships and a commitment to communicating consistently about Agency priorities and activities. These actions will make the Agency more effective as America’s Gatekeeper, protecting the nation’s global economic, intellectual, political, and military advantages.

Objectives

1

Build an integrated agency that operates holistically as a single enterprise.

2

Sustain a culture of innovation, strong partnerships, and inclusivity.

3

Raise external awareness of the DCSA mission and capabilities through proactive outreach and integrated stakeholder management to build broad partnerships with industry, government, and academia.

Enterprise Goal

Enable a productive work environment through mission-enhancing processes, policies, and automation. Merging multiple missions and related mission support functions into DCSA created numerous back-office challenges and opportunities. Today, DCSA business processes are largely stove-piped and paper-based with limited or sub-optimal information technology (IT) augmentation. Several of our functional and mission support offices are notoriously under-resourced. Every marginal dollar and person-hour spent in support of inefficient business processes is a critical resource that cannot be re-invested into DCSA's core mission.

To enable a more productive work environment, DCSA must scale its functional and mission support operations to meet the needs of this dynamic, multifaceted agency. DCSA will integrate and fully automate time-consuming back-office business processes to free its employees to exercise human judgement. The Agency will embrace a culture of continuous process improvement and apply business process re-engineering practices to prioritize and transform processes while rooting out waste. Service level agreements will be established, setting a gold standard for customer service and improving the customer experience.

IT platforms such as Enterprise Service Delivery will automate and integrate re-engineered end-to-end business processes. DCSA will leverage bots, robotic process automation, and artificial intelligence/machine learning to reduce costs and operate more efficiently, increase speed, improve accuracy, reduce errors, increase consistency, reduce risk, and enforce data-driven decision-making.

Objectives

1

Mature functional and mission support offices by scaling them to match DCSA's size and complexity and leveraging automation and process improvements as appropriate.

2

Enable employees to focus on critical mission functions by eliminating, automating, or transferring manual processes.

3

Implement a structured program to continuously improve mission performance, user experience, and enterprise efficiency.

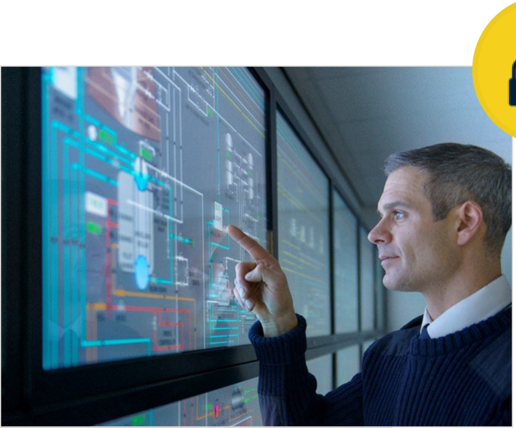
4

Reduce the administrative burden caused by internal policy and structures.

DIGITAL ECOSYSTEM

Enterprise Goal

Develop a secure digital ecosystem to align strategy, technology, data, and knowledge management to drive transformation and mission performance. The DCSA digital ecosystem is a mission-driven enterprise capability that relies on data-centric, cloud-based, and technology-agnostic investments to deliver a seamless digital experience across multiple platforms, systems, and services. Leveraging a zero-trust framework, the Agency will push traditional network boundaries – providing more secure and resilient digital protection capabilities while delivering seamless integration and optimal interoperability among internal and external mission partners, stakeholders, and customers. In addition, the Agency developed a data strategy and participates in the DOD Data Strategy Implementation Working Group. During the next five years, DCSA will transform into a data-driven organization.



DCSA will improve its decision-making capabilities by making data more readily available and optimizing knowledge and information sharing while improving information security. DCSA will implement augmented intelligence capabilities and assistive technologies as a workforce multiplier, shifting time spent on lower value-added activities to more complex challenges and priorities. The Agency's ability to deliver a robust digital ecosystem is constrained by fiscal realities that require an efficient and cost-effective investment portfolio; therefore, DCSA will leverage enterprise governance to prioritize investments in cloud, data, and technology capabilities that have the greatest return on investment.

Objectives

1

Align the enterprise architecture in support of the strategy by employing scalable solutions, integrating target DCSA IT systems including NBIS, and sunsetting legacy systems.

2

Implement a coordinated data strategy to unify data management for on-demand access and optimize data use enterprise-wide.

3

Create an adaptive cloud strategy in a zero-trust environment that enables flexibility and scalability.

4

Modernize IT capabilities to improve mission processes, create efficiencies, and provide sufficient security to protect our data.

RESOURCING PROCESSES

Enterprise Goal

Implement effective resourcing processes to enable DCSA leaders to align resources to priorities in near real-time. At its most basic, a strategy is nothing more than allocating an organization's resources to meet mission objectives. How an organization invests its energy, human capital, and financial resources is the most accurate indicator of its priorities. In that light, DCSA will adopt efficient and effective resourcing processes tied to this strategic plan. The Agency will align resources to priorities and continuously reallocate them as strategic priorities change.

The Agency will mature its resourcing processes, for example, by:

- Refining and improving its performance management framework, and adopting a set of leading, lagging, and outcome-based indicators that Agency leadership will monitor to ensure strategic goals are being met.
- Designing and executing a capabilities-based requirements process that will include the creation of a requirements council whose critical mandate will be to align requirements with missions, capability areas, and operational activities.
- Implementing oversight of the Component Acquisition Executive, responsible for all DCSA acquisition activities including reviewing and providing strategic direction for each IT program, assigning decision authorities, implementing the adaptive acquisition framework, standing up portfolios for service procurements, and developing a well-trained and diverse acquisition workforce.
- Transforming its financial management operations and processes to improve data-driven decision-making, and transparency in resource planning and execution, pricing for new products and services, and expansion of cost recovery mechanisms to support DCSA missions.

To meet the Agency's mission and enterprise goals, DCSA will establish a robust research and innovation program to integrate customer needs with state-of-the-art technical solutions by leveraging expertise within the Defense Innovation Marketplace (e.g., Federally Funded Research and Development Centers, University Affiliated Research Centers, and the Applied Research Laboratory for Intelligence and Security) and other established institutions such as the Critical Technology Protection Integration Center and the Defense Personnel and Security Research Center.

Objectives

1

Align resources to strategy and adapt to new mission sets via a strategic planning process, governance, and performance management.

2

Mature acquisition capabilities and processes across DCSA.

3

Expand the use of cost recovery mechanisms to structure the service catalog, manage demand, align investments, and organize services.

4

Generate and integrate innovation capabilities to deliberately advance agency mission objectives and keep pace with our adversaries.

5

Optimize facilities planning to modernize and streamline footprint.

STRATEGY IMPLEMENTATION AND MANAGEMENT

DCSA's strategy is not a static framework or aspirational words on a page. It is a portfolio of initiatives aligned to strategic objectives and goals. To execute the strategy, DCSA will:

- Establish the strategy execution team to monitor the implementation of the strategy, report on progress, escalate issues, and adjust efforts as needed.
- Operationalize the strategy through deliberate planning by each goal champion to identify requirements, resources, targets, and accountability for delivery.
- Launch deep dives on strategic priorities to jump-start execution of the strategy.
- Establish measures of success for each goal and track progress.

DCSA's strategy will continue to evolve as conditions change. To ensure that the strategy remains relevant, the Agency will follow these strategic planning practices:

- Implement an annual strategic review process that assesses changes in the operating environment and conducts scenario planning to understand how DCSA's mission and priorities may evolve into the future.
- Establish a resource reallocation process that regularly realigns investments with strategic priorities. This process will also determine what DCSA will not do. In a resource-constrained environment, DCSA must make hard decisions to ensure resources are appropriately applied in accordance with the strategy.

Finally, no strategy is complete on its own and DCSA has built an enterprise-wide governance strategy to streamline the Agency's operational and strategic decisions. The Executive Steering Council (ESC) will serve as the enterprise-level forum that deliberates and decides on Agency strategic direction and prioritization and provides oversight of key initiatives. The ESC will oversee changes to the strategy and be the body through which the goal champions will report progress and issues to DCSA leadership. The ESC will also be the forum that approves any changes to the portfolio of projects based on the annual Strategic Planning Process cycle results. The portfolio of projects will be reviewed and updated annually in advance of the planning, programming, budgeting, and execution process to inform DCSA's Program Objective Memorandum submission.

The goal champions will use the appropriate governance bodies to engage stakeholders in decision-making and report progress related to their implementation plans. DCSA governance is designed to advise and assist the DCSA Director as the Agency formulates and executes the enterprise strategy. It addresses mission operations, programs, enabling functions, and issues that affect the entire Agency. Strong governance allows the Agency to review the information and make well-informed, timely, and integrated decisions efficiently and transparently. DCSA will provide effective governance through participation at all levels with clear lines of communication, sound issue escalation mechanisms, and outcome-focused decision-making forums.

CONCLUSION

DCSA developed this strategy in collaboration with customers and external stakeholders. It is designed to align with broader intelligence and defense strategies while laying the foundation for a growing DCSA mission. This strategy represents a maturation from the transformation agenda that initially guided efforts to align merging organizations for the nascent Agency. Successful implementation of this plan will improve DCSA's capacity to accomplish our mission with excellence and unity of purpose.

DCSA is the Gatekeeper for both the USG and the DIB. The security of our nation depends on the success of DCSA's mission. This strategy represents an actionable plan to transform DCSA's mission performance while enhancing our national security by safeguarding America's sensitive information and trusted workforce.

ACRONYMS

CDSE	Center for Development of Security Excellence
CI	Counterintelligence
CUI	Controlled Unclassified Information
DCSA	Defense Counterintelligence and Security Agency
DIB	Defense Industrial Base
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DOD	Department of Defense
ESC	Executive Steering Council
FOCI	Foreign Ownership, Control, or Influence
IT	Information Technology
NBIS	National Background Investigation Services
NCCA	National Center for Credibility Assessment
NISP	National Industrial Security Program
OPM	Office of Personnel Management
TW	Trusted Workforce
USG	United States Government

REFERENCES

National Defense Authorization Act for Fiscal Year 2020, Section 847, "Mitigating Risks Related to Foreign Ownership, Control, or Influence of DOD Contractors or Subcontractors"

Executive Order 12829, "National Industrial Security Program," December 1993, as amended

Executive Order 13869, "Transferring Responsibility for Background Investigations to the Department of Defense," April 2019

DOD Directive 5105.42, "Defense Counterintelligence and Security Agency Charter" (draft)

DOD 5220.22-M, "National Industrial Security Program Operating Manual," as amended

The President's Management Agenda, November 2021

Interim National Security Strategic Guidance, March 2021

National Defense Strategy, 2018

National Military Strategy, 2018

National Intelligence Strategy, 2019

National Counterintelligence Strategy, 2020

Defense Security Enterprise Strategy, July 2021

Defense Intelligence Strategy, 2020 (classified)

27130 Telegraph Road | Quantico, VA | 22134
E-Mail: dcsa.quantico.dcsa.mbx.change-management--strategic-planning@mail.mil