



**Defense  
Counterintelligence  
and Security Agency**

DCSA at Five Years:

---

# Journey to Trust Through Transformation

# Table of Contents

Introduction.....	4
How We Got Here.....	5
Transition and Transformation .....	7
Driving Unity of Effort .....	9
Culture Transformation .....	9
Enterprise IT and Acquisition Transformation .....	10
Field Transformation.....	12
Industrial Security.....	16
Personnel Security .....	19
Security Training.....	23
Counterintelligence and Insider Threat.....	25
Evolution of Mission Support .....	29
Preparing for the Future Threat Landscape .....	32
Conclusion.....	33
Appendix: DCSA by the Numbers in FY24.....	34
Appendix: History of Legacy Agencies.....	35
Resources .....	37
Acronym List .....	38

## Director's Letter

Today we find ourselves operating in a rapidly changing environment marked by strategic competition among global powers, technological advancement and complex threats to the United States of America. Yet, I remain confident in our nation's future because our future is protected by the dedication of the Defense Counterintelligence and Security Agency (DCSA) and our partners.

I am honored to lead DCSA, the nation's largest security agency and provider of integrated security services for the Department of Defense and the federal government. I often say that trust — in people, facilities, technology and information — anchors our mission. The trust DCSA has built, and continues to build, is responsible for our transformative journey over the past five years.

Successfully merging unique legacy organizations to form DCSA has been not only an extraordinary undertaking, but a critical measure in our pursuit of full mission performance. I believe that this integration — and more crucially, the unification — of efforts is the foundation that will prepare our agency to drive increased efficiencies in security services as the federal government goes through a broader transformation.

As we look ahead, we are fully aligned with the priorities of the Secretary of Defense to rebuild our military capabilities to meet emerging threats by reviving the defense industrial base, leveraging new technologies and reforming the acquisition process. DCSA plays a critical role in ensuring that trust enables these advancements — whether through safeguarding supply chains, mitigating security risks or supporting efforts to streamline acquisition for new defense companies. The defense landscape is evolving, and our agency must evolve with it, reinforcing the trust that underpins national security.

While this report details our origins, DCSA's 2025-2030 Strategic Plan is a roadmap for the path forward. Over the next five years, we will continue to strengthen/build the bridge between our history and our aspirations by deepening our focus on unifying efforts across missions, fostering collaboration with partners, enhancing our role in fortifying the industrial base and ensuring the swift adoption of cutting-edge technologies.

We will continue to focus our vision to be the premier provider of integrated security services, working together to strengthen our capabilities, modernize our approach and uphold the trust that is the foundation of our national security mission. I encourage you to reflect upon, and take pride in, our impressive achievements over the last five years. DCSA is proud to help uphold America's strategic military advantage and ensure that the U.S. military remains the strongest in the world.


The proud men and women of DCSA continue their unwavering commitment to defending this country. I look forward to their continued excellence and innovation that will safeguard tomorrow, today.

Sincerely,



**David M. Cattler, Director, DCSA**





## Introduction

DCSA is the U.S. government's largest integrated security services provider and the only purpose-built security agency. While DCSA operates largely out of the public eye — DCSA plays a significant and foundational role in the national security framework and has a direct and personal impact on the government personnel and industry partners who contribute to America's national security. DCSA is in the business of trust — establishing it, sustaining it and building upon it to protect America's competitive edge.



Without trust in our workforce, our facilities, our data and Information Technology (IT) systems, achieving national security objectives would be impossible.

Trust enables our military and industrial base to build capabilities, drive innovation and uphold America's military and economic strength. As a service provider, DCSA is committed to handling every interaction with customers and stakeholders with the utmost integrity, transparency and respect.

### Today's DCSA:

- Delivers a trusted federal workforce and ensures that trust is maintained through initial vetting and Continuous Vetting (CV) services.
- Implements the National Industrial Security Program (NISP) for the Department of Defense (DOD) and 35 federal agencies.
- Protects the Defense Industrial Base (DIB) from insider and foreign entity threats through counterintelligence functional services and insider threat support.
- Delivers world-class security training and credentialing services to DOD and the security enterprise.

Since its formation in 2019, DCSA has taken on new missions, adapted to shifting demands and transformed internal processes, all while reinforcing its core values and prioritizing employee engagement. In its fifth year, the agency's workforce of nearly 15,000 federal employees and contractor personnel conduct integrated security operations around five core mission directorates: Personnel Security (PS), Industrial Security (IS), Field Operations (FO), Counterintelligence and Insider Threat (CI) and Security Training (ST).

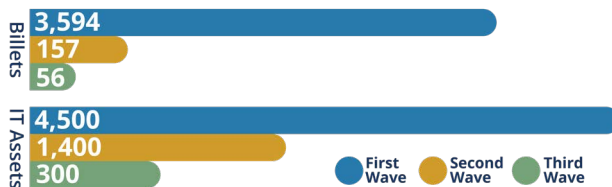


## How We Got Here



This document provides a retrospective of the past five years, including a look at the agency's formation, its transformational journey, an overview of each mission area and DCSA's work to prepare for the future threat environment.

DCSA was established October 1, 2019, in response to legislative and executive action that followed a massive data breach in 2016. The Fiscal Year 2018 National Defense Authorization Act (NDAA) required the phased transfer of DOD Background Investigations (BI) from the Office of Personnel Management (OPM) to the Defense Security Service (DSS). The size and complexity of DCSA's security missions today is a result of three waves of agency integration (e.g., the National Background Investigations Bureau (NBIB), the DOD Consolidated Adjudications Facility (DOD CAF), DSS and the transfer of select functions from the Defense Information Systems Agency (DISA), the Defense Manpower Data Center (DMDC) and similar agencies). DCSA is now composed of mission areas and functions from eight agencies.



**First Wave:** The Secretary of Defense (SECDEF), in January 2019, placed the DOD CAF under the authority, direction and control of DSS with an effective date of October 1, 2019. The Secretary also directed that DSS be renamed DCSA to more accurately reflect its changed missions. Executive Order (EO) 13869, signed on April 24, 2019, directed DSS to assume the primary responsibility of conducting the background investigation mission for the federal government and transferred NBIB from OPM to DSS. These actions brought together the PS and IS missions and established DCSA as the largest dedicated security agency in the federal government. Additional mission transfers included their respective training components — the Center for Development of Security Excellence (CDSE) and the National Training Center (NTC).

**Second Wave:** Effective October 1, 2020, DISA and DMDC transferred select missions to support DCSA's security services, including the National Background Investigation Services (NBIS). This transfer included IT systems and associated functions, personnel and resources supporting the Defense Personnel Security Enterprise. DCSA also assumed responsibility for the maintenance and operation of legacy IT systems from OPM that support the background investigation mission.

**Third Wave:** Effective October 1, 2021, the National Center for Credibility Assessment (NCCA) transferred from the Defense Intelligence Agency (DIA) to DCSA.





The DCSA seal was created to represent the key missions and functions of the agency. The portcullis, a massive metal gate used to protect and secure castles during times of attack, symbolizes DCSA's mission to defend the nation. The eagle, a symbol of the United States, is in flight, lifting and lowering the portcullis using its chains, which illustrates the gatekeeping

function of the organization — either denying or granting entry to the continuous flow of classified information, materials, technology and personnel seeking access to federal agencies. It's from the portcullis, or gate, that the agency adopted 'America's Gatekeeper' as an early slogan.

*"This merger offers an unparalleled opportunity to streamline our security clearance program, maintaining our military advantage in an era of complex, global threats."*

**Kari Bingen**, Principal Deputy Under Secretary for Defense for Intelligence (PDUSD(I)) (2017-2020)

## Transition and Transformation

Shortly after its inception in 2019, DCSA developed and introduced an operating model (OpModel) that provided alignment and integration of the work of multiple, formerly independent agencies within the new, unified agency. The OpModel laid the foundation for the agency's continued transformation and led to its key early accomplishments. These included stand-up of FO as a separate mission; establishment of a continuous process improvement program to drive benefits in mission area cost, quality and timeliness; and execution of the Working Capital Fund (WCF) to inform cash balance management processes. It also provided a foundation to set the agency on the path of a new five-year strategic plan. The OpModel and initial strategies were based on a set of design principles that guided the maturation of DCSA. They also moved the agency to be integrated and risk-based in its organization and mission operations; to be automated, standardized and cost-conscious in its business operations; and focused on customers in its service delivery.



**Mission:** Through vetting, industry engagement, education, CI support, secure the trustworthiness of the United States government's workforce, the integrity of the cleared contractor support, and the uncompromised nature of its technologies, services, and supply chains.

**Vision:** DCSA is America's Gatekeeper: safeguarding the nation as the premier provider of integrated security services — national security is our mission; people are our greatest assets.

### DESIGN PRINCIPLES

#### PROCESSES

Manual > Automated

#### OPERATIONS

Compliance > Risk-based

#### ORGANIZATION

Siloed > Integrated

#### SERVICES

Ad-hoc > Standardized

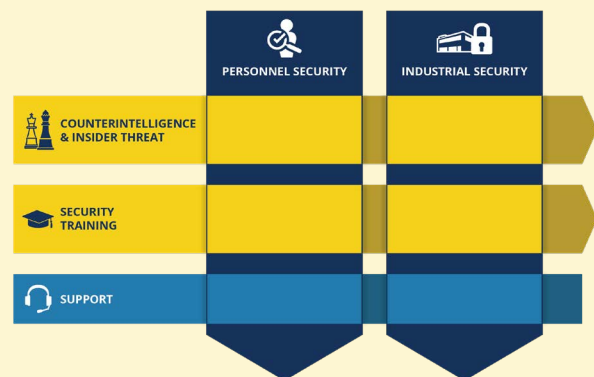
#### METHODS

Resource-intense > Cost-conscious

#### FOCUS

Agency > Customer

### DCSA OPERATING MODEL












A clear articulation of how an organization's capabilities come together to perform work and deliver value.

### STRATEGIC PLAN

The mission and enterprise goals DCSA will work toward in the next five years through transformation project implementation, mission integration and effective progress management



Industrial Security	Personnel Security	CI and Insider Threat	Security Training
 <p><b>Enable threat reduction and mitigate vulnerabilities</b> to classified and sensitive information and technology in the U.S. industrial base</p>	 <p><b>Identify and mitigate personnel-based threats</b> while enabling customers to onboard talent quickly</p>	 <p><b>Identify, integrate, and share threat information</b> across the enterprise to help drive risk-based, data-driven decisions and actions</p>	 <p><b>Train U.S. Government, industry, and Agency personnel</b> to mitigate risk in support of national security</p>
 <p><b>Recruit, develop, engage, and retain</b> a talented and high-performing workforce able to meet the demands of our evolving mission</p>			
 <p><b>Unify efforts across mission areas</b> within DCSA by building a shared agency culture focused on public service and our nation's security</p>			
 <p><b>Enable a productive work environment</b> through mission-enhancing processes, policies, and automation</p>			
 <p><b>Develop a secure digital ecosystem</b> to align strategy, technology, data, and knowledge management to drive transformation and mission performance</p>			
 <p><b>Implement effective resourcing processes</b> to enable DCSA leaders to align resources to priorities in near real-time</p>			

DCSA's inaugural five-year strategic plan, released in 2022, described desired outcomes and specific actions DCSA would need to accomplish to achieve its mission in an evolving threat landscape. DCSA identified nine goals — four mission goals and five cross-cutting enterprise goals. All nine goals were necessary and mutually supporting. This strategic plan provided a framework to guide DCSA leaders on their transformation journey for each of DCSA's four missions and to expand the capabilities of the support and enabling functions. DCSA's transformation activities were undergirded by efforts to drive Unity of Effort (UoE), mission integration and information sharing across DCSA and with its DOD and federal customers, industry partners and oversight stakeholders. Only through UoE, could DCSA realize its vision to be the premier provider of integrated security services.

### STRATEGIC PLAN 2022-2027



Defense Counterintelligence and Security Agency

*The strategic plan was not built from scratch. After DCSA's inception in 2019, the agency built a future state OpModel, and the strategic framework to provide the interim guidance needed to align and prioritize transformation initiatives while merging organizations . . . The DCSA strategic plan will be the "center of gravity" as the agency monitors key performance indicators, resource requirements, transformation initiatives and other key components of its operations."*

**Wally Coggins**, Chief Digital and AI Officer (Chief Strategy Officer 2021-2024)





## Driving Unity of Effort

### Culture Transformation

DCSA was established by merging multiple entities into one, and each legacy organization brought with it its own distinct culture. Melding the organizational cultures from these distinct legacy entities into a unified and common culture was paramount to DCSA becoming the premier provider of integrated security services to protect our nation's most sensitive information. As a result, agency leaders prioritized activities focused on agency culture and brought organizational changes in the field and in the mission support functions to drive UoE across the agency.

DCSA leadership took deliberate steps to build a common culture based on DCSA's values — mission, people, service, integrity and innovation — and the agency's role in national security. The agency conducted several dedicated activities to engage the workforce and grow this common culture to include a culture survey and UoE Roadshow. After listening to the workforce, the leadership team committed to an UoE Action Plan that was published in May 2023 and was built to address pain points identified by employees and defined high-impact activities for prioritizing people and unifying organizational culture. All 32 UoE Action Plan activities have achieved visible progress since the plan's establishment.

*The role we play in securing the trustworthiness of the United States government's workforce and protecting our nation's critical assets is indispensable to this fight. We, as Gatekeepers, are coming together as one entity with a unified culture, to manage the threats as they come to us."*

**Daniel Lecce**, Deputy Director

### UoE and Culture Survey and Roadshow

The UoE and Culture survey was shared among DCSA's workforce to collect input around the agency's culture. The survey led to direct employee engagement and valuable feedback. The survey was followed by a UoE Roadshow where DCSA's Deputy Director, Daniel Lecce engaged face-to-face with employees across the country. These efforts resulted in the accomplishment of short-term, high impact activities that yielded positive change and a more cohesive DCSA employee experience.

#### UoE initiatives included:

- A mid-level leadership program to train/ educate future leaders on tools and techniques for improving communications both laterally and to subordinates as part of the Leadership Development Program (LDP).
- An Onboarding Program Management Office in the Human Capital Management Office (HCMO) streamlining the onboarding process for new hires.
- A 179-day Career Broadening Program to provide DCSA employees with opportunities to work in different directorates.

## DCSA Values

**Committed to Mission:** Ensuring national security is at the forefront.

**Invested in People:** Valuing and supporting our team.

**Passionate about Service:** Dedication to serving our country and partners.

**Unwavering in Integrity:** Acting with honesty and accountability.

**Driven to Innovate:** Continuously evolving to meet emerging challenges.



## Enterprise IT and Acquisition Transformation

Since its inception, DCSA took several steps to mature its organizational capacity to manage and build a portfolio of enterprise-wide IT programs and to meet the DOD acquisition oversight standards. The DCSA Program Executive Office (PEO) was formally established October 1, 2020, and its creation marked the first milestone in the maturation evolution of DCSA's IT transformation, establishing a unified capability to oversee and enhance the agency's portfolio of enterprise-wide IT programs. As DCSA assumed responsibility for multiple IT acquisition programs, it became clear that a dedicated office was needed to align these initiatives under a single framework, ensuring efficiency, accountability and adherence to best practices. In early January 2025, PEO held its fifth ceremony to charter the Cloud Services and Mission Operations program.

The PEO employs DOD acquisition best practices to design, develop, test, deploy and secure mission-critical systems that serve DOD, the U.S. government and cleared industry. Its work spans a

range of functions, including BI, national IS, security education and insider threat management. The PEO also oversees innovative programs in areas such as intelligence analytics, robotic process automation, cloud services and cybersecurity. The PEO is integral to DCSA's evolution, delivering integrated solutions that advance the agency's mission and support its enterprise-wide capabilities. PEO oversees their cybersecurity service in support of the enterprise cybersecurity program under the agency's Chief Information Security Officer (CISO).



In 2023, DCSA stood up the Component Acquisition Executive (CAE) to provide comprehensive and dedicated oversight of the PEO IT programs and meet the DOD acquisition policy requirements. Over the years, the CAE helped mature PEO's acquisition workforce and provided oversight to eight PEO programs. The maturation of the CAE set the foundation for DCSA to embrace Enterprise Scaled Agile Framework (SAFe) principles not only in the PEO, but as an agency.

In November 2024, at DCSA's second Acquisition Workforce Symposium, Director David Cattler, DCSA's CAE, signed the agency's Call to Action establishing the Enterprise Lean-Agile Center of Excellence (LACE) which will be responsible for defining and guiding the implementation of an Enterprise SAFe Operating Model (ESOM) aimed at enabling the efficient, secure and controlled delivery of high-quality, mission-enabling technology solutions at scale. By the end of 2024, 264 DCSA employees completed agile training, with 178 passing the certification exam, helping to achieve the Director's vision of developing an agile mindset at every level.



**264** DCSA employees completed agile training, with **178** passing the certification exam

*As of the end of 2024*

Symposium speakers included Assistant PEO and the Acquisition Innovation Director, U.S. Army, Aric Sherwood and performing the duties of Assistant Secretary of Defense for Acquisition, Gary Ashworth. As the keynote speaker, Ashworth emphasized the importance of such events in fostering continuous learning, upskilling and acquisition knowledge sharing across DOD. "We must prioritize training and development within the acquisition workforce. At my level, we work closely with agencies like the Defense Acquisition University (DAU) to ensure that we're providing the right tools and training to support the ever-evolving needs of the acquisition community."



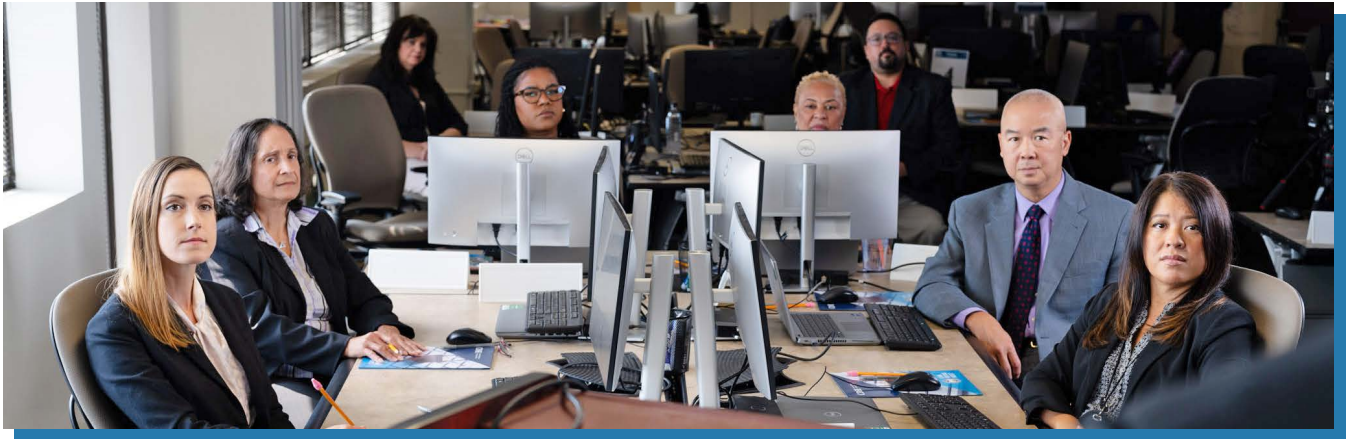
**DONNA LOGSDON ON THE IMPORTANCE OF ACQUISITION PLANNING AND RIGOR TO OUR SUCCESS ON ENTERPRISE-LEVEL IT PROJECTS**

*"The role and importance of acquisition rigor and the development of the acquisition workforce has a direct impact on DCSA's mission success. The continued development of the acquisition workforce will enable the agency to deliver mission capabilities at the speed of need. The role of the acquisition professional cannot be understated in value to this endeavor. The role of the CAE, and by extension the CAE staff, is to provide the opportunity for acquisition personnel to get the training they need to do their job; provide them with the strategic guidance and support needed to establish a program baseline; and monitor progress against that baseline in a data-driven manner to provide our senior level decision makers what they need to make strategic decisions that will enable mission success."*

**Donna Logsdon**, Component Acquisition Executive Staff



## Field Transformation



When DCSA was established in 2019, legacy agencies had their own unique structures and siloed field organizations. The NBIB field offices were organized into three regions, while DSS was divided into four regions — leaving DCSA and its field offices without clear regional boundaries.

DCSA leadership immediately recognized the need to unite the field offices — as well as their respective operations and staff — and set out to create an organizational structure that would break down legacy siloed organizations and lead to more UoE across the field. Given the size and nature of the field work, the goal of aligning all missions to one regional structure was a significant step towards this goal. In addition, a holistic approach to field locations provided an opportunity to consolidate offices and achieve cost savings.

*The new regional organizational structure under FO is part of our enterprise initiative to integrate DCSA's different missions and operational cultures into one cohesive organization. It is driving consistent application of policies related to space, vehicles, supplies, IT and general resourcing across the missions. It will also lead to improved mission effectiveness through integration across regions and missions."*

**Larry Vincent**, Assistant Director, Field Operations

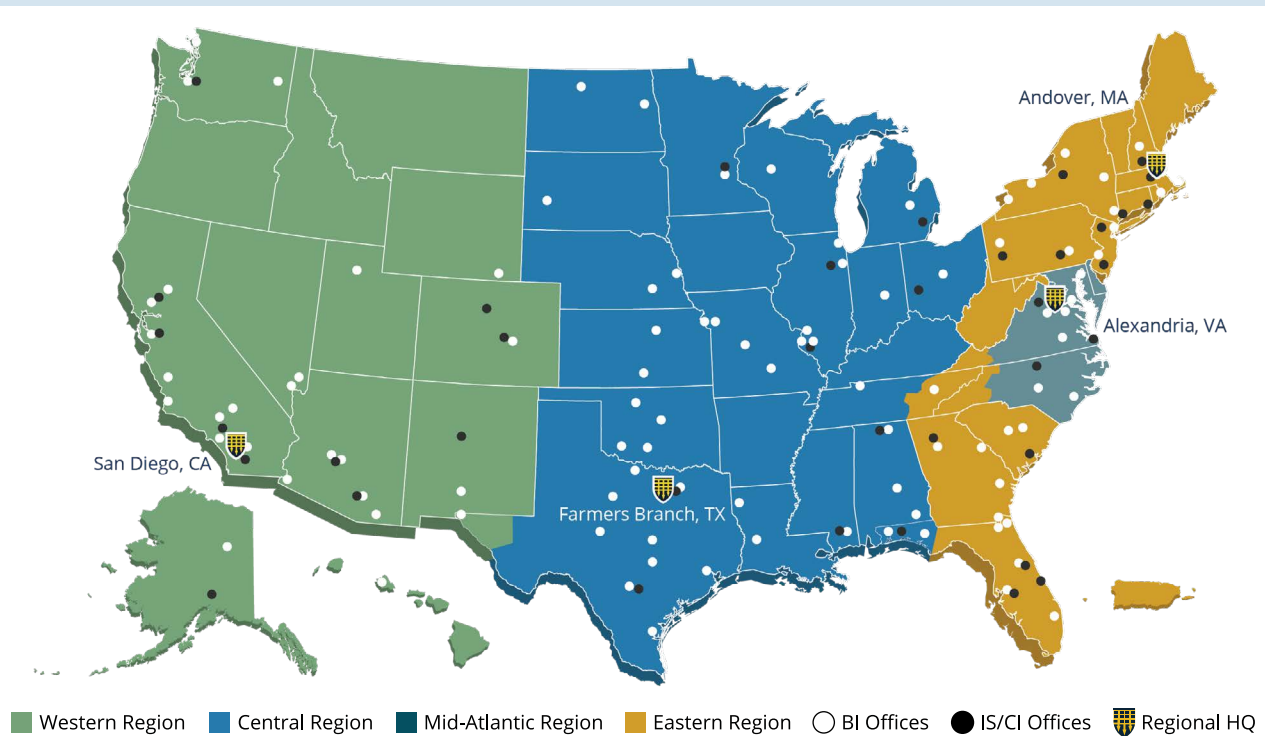
DCSA reorganized its FO into four regions with the location of each regional headquarters selected based on their proximity to customers, industry partners and government stakeholders. This new FO structure and the formal creation of the FO directorate signified the agency's dedication to driving coordinated action, efficiency in support functions and standardization across the field workforce. As a result, support to operations in the field were better aligned to FO mandates and structure.



## DCSA Regional Headquarters

**Central Region:** Farmers Branch, Texas  
**Eastern Region:** Andover, Massachusetts

**Mid-Atlantic Region:** Alexandria, Virginia  
**Western Region:** San Diego, California



In addition to actions taken on specific cases, one of the pilot benefits has been building the foundation for integration, both from a process and culture perspective, that will ultimately enable the agency to utilize mission authorities, operations and data to better inform the threat picture across industry and the federal enterprise.”

**Justin Walsh**  
Regional Director, Mid-Atlantic Region

### Mission Integration Pilot

The central goal of the Mission Integration Pilot conducted by the Mid-Atlantic Region was to foster collaboration and create repeatable processes to support mission integration in the field. At its core, the pilot sought to unify efforts across IS, BI, Cybersecurity and Counterintelligence while mitigating risks and ensuring a cohesive approach to safeguarding national interests.



DCSA's efforts to consolidate and reorganize the field workforce were strategic, deliberate and data-driven; and quickly saw positive impacts. Under the new structure, the agency's PS, IS and CI missions were integrated under FO, increasing recruiting, reducing attrition, improving information sharing and providing transparency across missions.

DCSA ensured that enabling functions were adequately deployed and disseminated across its field locations and hired specialists in emergency management, physical security, anti-terrorism and force protection, general security and information technology across all regions. These actions removed a significant administrative burden from the gatekeepers executing the mission in the field.

### Celebrating DCSA's Newest Regional Headquarters

In June 2024, DCSA opened its new Central Region headquarters in Farmers Branch, Texas. The event was marked with a ribbon cutting ceremony attended by key members of DCSA leadership, local government officials, members of Congress and federal partners.



*As regional director, I can tell you what you are seeing, what you are hearing, where you are sitting, represents a transformative process for DCSA. It is an evolution in our agency, a vision that has materialized."*

**Roy Hawkins**, Regional Director, Central Region

While more than 60 DCSA employees will work from the new headquarters, the facility will support over 700 DCSA personnel across 20 states, helping to streamline operations in PS, IS, CI and ST.

In addition to opening a new regional headquarters, DCSA also established several new field offices across the country to support field personnel by reducing the geographic area they are responsible for and to allow for closer coordination with records providers.

While FO helped drive mission integration and a unified culture, the agency's core mission directorates continued to execute with a keen eye on internal transformation in support of the agency's larger transformation goals.

### Engagement with Industry

With the stand up of FO, DCSA placed a senior leader in each of the regional headquarters to bring DCSA leadership closer to our industry partners across the country. In 2023, DCSA started hosting industry conferences in each of the regions to provide a forum for information sharing and collaboration to strengthen the partnership with industry to help counter the evolving threat.



### Did You Know?

Watchtower is a PS-designed application designed to provide BI field agents with the “right” information with efficiency and agility. The application allows agents to focus on issues while briefing cases, rather than on re-writing case information resulting in significant time savings.



## Industrial Security

Partnering with industry to maintain trust in America's workspaces and classified technologies

*Without security safeguards, critical technology can end up in the hands of our adversaries, eroding our nation's military and economic competitive advantages. The threat is real and as a whole of government effort, be ready."*

**Matthew Redding**, Assistant Director, Industrial Security

DCSA's IS mission protects national security by clearing industrial facilities, personnel and associated classified information systems. DCSA serves as the primary interface between the federal government and industry, providing daily oversight, advice and assistance to cleared companies and determining the ability of those companies to protect classified information.

DCSA administers the NISP on behalf of DOD and 35 other NISP signatory federal departments and agencies. Through the NISP, DCSA ensures that sensitive and classified U.S. government and foreign government information, technologies and material entrusted to cleared industry are properly protected.

DCSA does this by performing entity risk identification, analysis and management services; by vetting companies for foreign ownership, control or influence (FOCI); and by reviewing business integrity and lawful conduct risk indicators to protect government information and technology. DCSA also oversees the risk management framework (RMF) assessment and authorization (A&A) process, and validates that safeguards are effectively employed to protect the national security systems. DCSA is responsible for approximately 5,500 classified contractor information systems registered within

its database of record, the NISP Enterprise Mission Assurance Support System (eMASS).

Over the past five years, the IS mission transformed in multiple ways to implement new policy guidance, improve and increase the efficiencies of its processes and to mature and improve DCSA's relationship with its industrial base partners. The following are just some of the achievements in the past five years in IS:

**New Policy Guidance:** A major transition in the oversight of the NISP occurred with the move from a DOD manual to a federal rule: 32 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM). DCSA IS personnel successfully planned, coordinated and managed the transition for over 10,000 cleared companies with 13,000 cleared contractor facilities. The new rule also included several new program requirements that required DCSA to provide relevant guidance and a full suite of communication tools.

**Process Improvements:** A facility clearance is the entry for a company or academic institution to join the NISP. IS combined a few smaller offices, leveraging key research and analysis capabilities, to form a larger Entity Vetting office to improve the facility clearance process and decrease any processing timelines.



DCSA successfully developed the Security Rating Scorecard in collaboration with the National Industrial Security Program Policy Advisory Committee (NISPPAC) Industry Working Group. This scorecard introduced a numeric security rating score and enhanced criteria definitions, addressing industry requests for greater clarity and consistency. The scorecard was successfully implemented in October 2024.

**Relationship with Stakeholders:** IS personnel implemented an intentional communication strategy to foster stronger collaborative relationships with industry and government stakeholders through a wide range of engagements. One such event was the inaugural NISP Executive Signatory Conference, gathering senior leaders from the 35 NISP signatory agencies that receive DCSA security services. The conference aimed to address current security challenges, reaffirm the program's core principles and establish a clear vision around DCSA's 2040 strategic goals.

**New Capabilities:** In December 2023, DCSA renamed the NISP Authorization Office to the NISP Cybersecurity Office to properly align with the broader scope of cybersecurity responsibility of the NISP mission. A component of the increased



cybersecurity responsibilities was to create a classified cloud environment for industry. DCSA partnered with the Under Secretary of Defense for Intelligence and Security (USD (I&S)), DISA and cloud vendor to pilot a pathway for NISP contractors with contractual requirements to take advantage of cloud offerings.

DCSA also established dedicated Cyber Operational Readiness Assessment (CORA) teams which led to increased assessments for those NISP contractors with approval to connect to the Secret Internet Protocol Router Network (SIPRNet). The increase, from 15-20 per year to a projected 75, will raise senior level visibility and cyber readiness into warfighter networks.

### On the Horizon:

**Section 847:** A new DOD policy was issued to implement Section 847 of the NDAA for Fiscal Year 2020, DOD Instruction 5205.87, "Mitigating Risks Related to Foreign Ownership, Control or Influence of Department of Defense Contractors or Subcontractors." Section 847 expanded DCSA's review and assessment of FOCI risks to apply to any DOD-contracted companies with contract values exceeding \$5 million that are not purely commercial in nature.

This is a major reform to DOD acquisition policy, and DCSA will be ready to support this mission when the new Defense Federal Acquisition Regulation rule is published and added to applicable DOD contracts and subcontracts. To comply with the new requirements specified by Section 847, DCSA is developing and implementing a program based on current facility clearance and FOCI functions within the NISP to vet the foreign interest risk of all applicable contractors and subcontractors.



## Did You Know?

**NAESOC:** The National Access Elsewhere Security Oversight Center (NAESOC) was established to provide consistent security management for select “access elsewhere” (AE) facilities that do not possess classified information onsite. Of the 12,000 cleared facilities that DCSA oversees as part of the NISP, approximately 8,000 are categorized as AE facilities.

**AA&E:** DCSA is responsible for ensuring that contractors that manufacture, test, store or transport sensitive arms, ammunitions and explosives (AA&E) on behalf of DOD comply with all physical security requirements.

**ISP:** DCSA's International and Special Programs (ISP) oversees and manages classified information responsibilities with foreign governments, contractors and the North Atlantic Treaty Organization (NATO). Among other responsibilities, ISP facilitates and supports the coordination of international reciprocity visits. DCSA shared industrial security best practices with approximately 12 countries over the years including Australia, Israel, Singapore, India, Bangladesh, Japan, Philippines, Belgium, France, Korea, New Zealand and Taiwan.

DCSA met with its Australian counterparts and discussed unclassified and classified topics related to technology, threat actors, cybersecurity, security training and personnel security that will shape the Australia and U.S. partnership in the coming years.



## MISTY CRABTREE ON LEADING COLLABORATION WITH INDUSTRY FOR THE SCORECARD

*“In my role as a NISP Mission Performance (NMP) project manager, I had the privilege of leading a high-impact initiative focused on improving the security rating process. By prioritizing collaboration and fostering strong relationships with internal stakeholders and industry partners, we jointly developed a forward-thinking solution that minimized subjectivity and enhanced process efficiency, consistency and productivity. To do this, we established two working groups — an internal agency working group to leverage field expertise and drive process enhancements, and a NISPPAC working group to gather real-time industry feedback on those enhancements. For over a year, I worked closely with both working groups, facilitating a rich exchange of ideas and tapping into collective expertise. This collaborative approach yielded a streamlined process and optimal outcomes for all involved parties, earning praise as a paradigm of partnership. The resounding success of this endeavor inspired DCSA to adopt this collaborative model for future process improvements, setting the stage for continued innovation and excellence.”*

**Misty Crabtree**, Senior Action Officer, NISP Mission Performance Division







## Personnel Security

Vetting and establishing trust in America's federal and contractor workforce

*Synergy and effectiveness is first and foremost in the complicated processes of conducting BI, adjudications and vetting. Prior to my arrival, each of these organizations were hugely successful on their own, but I think together they are even stronger. By working together, we are more proficient and we have the opportunity to be even better."*

**Dr. Mark Livingston**, Assistant Director, Personnel Security

DCSA's PS mission delivers efficient and effective BI, CV and adjudications to safeguard the integrity and trustworthiness of the federal and contractor workforce. DCSA's end-to-end personnel vetting process ensures an exhaustive review of cleared personnel and complements the PS and insider threat activities.

DCSA is the federal government's largest Investigative Service Provider (ISP) and primary implementer of vetting reform under Trusted Workforce 2.0 (TW 2.0). DCSA is responsible for 95% of national security clearance decisions in the federal government.

In addition, in 2024, DCSA began the phased implementation of CV services for the Non-sensitive Public Trust (NSPT) population. The NSPT population includes individuals who hold non-national security roles but could pose a higher risk of damage to the integrity or efficiency of the workforce through misconduct. This initiative will see more than one million additional personnel enrolled in CV services.



### RYAN DENNIS ON INTRODUCING NEW PERSONNEL VETTING PRODUCTS & SERVICES

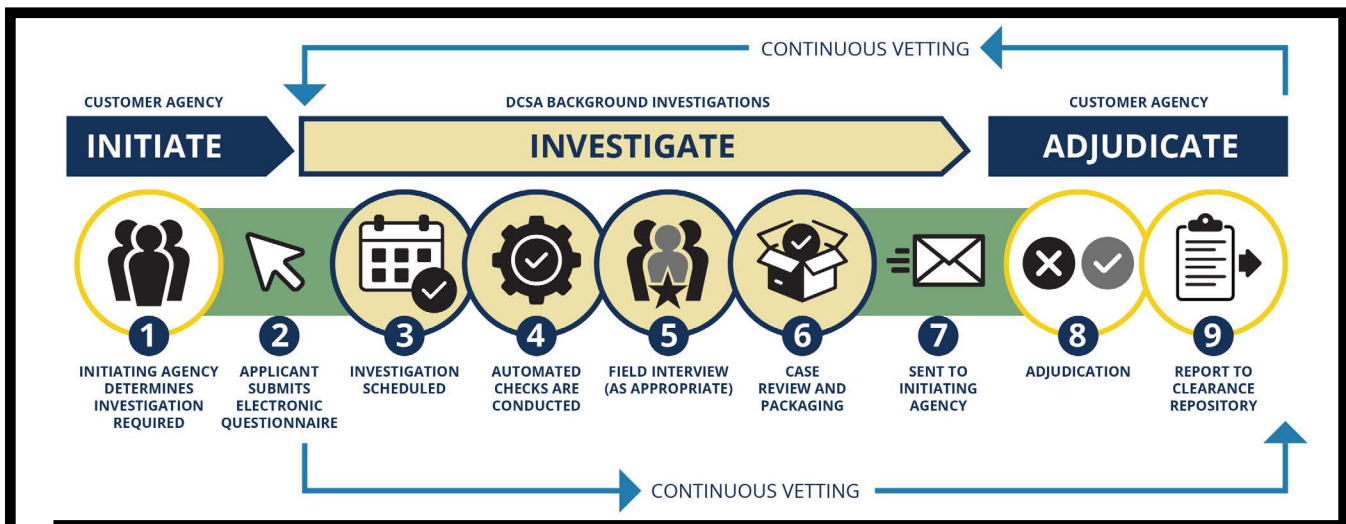
*"I'm honored to work beside our team of professionals who are taking an active role in making historic changes in personnel vetting. One of these being CV of the Public Trust population. The Public Trust population works with information the U.S. government has determined to be either moderate or high risk for preserving the confidence of the American people in our government. We worked diligently to establish the essential infrastructure needed to begin onboarding federal departments and agencies and enrolling this new population into automated data checks to enable near-real time risk identification. We then work with our customers to gather sufficient information to determine the ability to successfully rehabilitate and maintain confidence in the individual to preserve the trust of the public."*

**Ryan Dennis**, Deputy Assistant Director, Adjudication and Vetting Services



Led by the Performance Accountability Council's Program Management Office (PAC PMO), TW 2.0 is a government-wide reform effort that aims to transform the personnel vetting process by eliminating periodic reinvestigations in favor of CV. In addition to ensuring a trusted workforce in near-real time, TW 2.0 will also allow reciprocity across organizations and generate cost savings across agencies. TW 2.0, once adopted, is expected to change how the government establishes and maintains trust in the workforce with a continuous risk assessment model enabled by a new end-to-end suite of technology to meet the dynamic needs of the 21st century in support of the national security mission.

Since its inception, DCSA has worked towards full government-wide adoption of TW 2.0 using a phased approach with two key milestones: Trusted Workforce 1.25 (TW 1.25) and Trusted Workforce 1.5 (TW 1.5). DCSA began enrolling DOD and select federal agencies in an initial version of CV as part of TW 1.25, deferring traditional reinvestigations for automated record checks. TW 1.5 expanded on TW 1.25 by continuously checking individuals' backgrounds against seven additional sources comprising of eligibility, terrorism, criminal activity, foreign travel, suspicious financial activity, credit bureau and public records. TW 1.5 also leverages agency-specific records including self-reported information or investigative work conducted by local law enforcement.



### Did You Know?

DCSA conducts over 2.6 million background investigations annually (consisting of over 17.7 million record checks) to assess individuals for classified or sensitive roles, ensuring national security and public trust standards are met.

DCSA maintains the largest adjudication capability in the federal government and serves all three U.S. government branches. In FY24, DCSA rendered approximately 622,000 adjudicative decisions.

## National Background Investigation Services



In 2018, the TW 2.0 initiative was created to reform “personnel vetting” and how the government determines workforce trustworthiness. The effort

is managed through the Security, Suitability, and Credentialing Performance Accountability Council (PAC), established under EO 13467. The TW 2.0 initiative is now in its final phase of implementation.

To successfully implement TW 2.0, the delivery of NBIS, a personnel vetting IT system, is critical. NBIS is an end-to-end personnel vetting system that will be used by the DOD and over 100 federal agencies to achieve the TW 2.0 milestones.

In October 2020, the NBIS program was moved from DISA to DCSA. While the NBIS program met a major milestone to move the customer base to a new case initiation capability called Electronic Application (eApp), NBIS also faced numerous challenges that hampered progress and delivery over the years resulting in overall cost increases. DCSA made DOD oversight aware of these challenges in December 2023.

In 2024, new leadership at DCSA with sponsorship from the Office of the USD I&S, and milestone decision authority from the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD A&S), led the program through recovery sprints resulting in:

- The establishment of new requirements governance.
- An approved updated requirements baseline.
- An approved technical approach for NBIS digital transformation.
- Elevation of NBIS’ cybersecurity profile, and;
- A restructured NBIS program office through collaboration with the DOD Chief Information Officer (CIO).

These changes culminated in the release of an updated NBIS product roadmap aligned with the TW 2.0 implementation strategy.

These are significant milestones for DCSA as a High Impact Service Provider (HISP) with NBIS being the most impactful personnel vetting service to be provided in the federal government and industry.

Over the past five years, the PS mission transformed to better posture itself to implement TW 2.0, support NBIS development and improve engagement with customers. Simultaneously, PS is delivering the personnel vetting mission at scale to customers across the federal government, including in the post-COVID environment characterized by significant increase in demand for all TW 2.0 services.

### **Customer Engagement through Transition to**

**NBIS:** An Applicant Knowledge Center (AKC) was established to support applicants with application initiation questions related to the new eApp and legacy Electronic Questionnaires for Investigations Processing (e-QIP) form. The AKC was a new service for customers who had previously provided support of their own applicants. In November 2024, all DCSA customers moved successfully to eApp to initiate background investigations. Its intuitive design makes the application process easier to use for applicants.

Agency liaisons serve as the primary point of engagement with personnel vetting customers. Liaison engagements with federal customers, agencies and stakeholders have ensured a smooth transition to NBIS during the onboarding process and to educate customers on changes or updates related to PS processes and policies.

**Improved Quality:** PS implemented a government-wide Quality Assessment and Reporting Tool (QART) that enables customer agencies the ability to evaluate the quality of DCSA background investigations. Implementation of the tool has resulted in accurate and reliable metrics.

**HISP:** In December 2023, DCSA was designated a HISP by the Office of Management and Budget (OMB), underscoring DCSA's critical role in the federal security clearance process. This designation commits DCSA to enhancing the customer experience, streamlining the security clearance application process and building public trust through targeted improvements, aligned with federal goals for equitable service delivery.

### **On the Horizon:**

**New Products and Services:** The PS mission will continue to expand its TW 2.0 service offering to customers. By the end of Fiscal Year 2025, DCSA is projected to enroll up to one million members of the non-sensitive trust population across the federal government into continuous vetting.

In December 2024, DCSA began to implement reforms to the Security Review Proceedings (SRP) in support of due process and appeals for military service members, DOD civilians and contractor personnel whose eligibility for access to Sensitive Compartmented Information (SCI) is adjudicated by DCSA. The changes were directed by the USD I&S and are part of an ongoing effort to transform the department's PS review processes which determine eligibility for access to classified information or to occupy a national security position. The goal is to make the process transparent, person-focused and courteous.



## Security Training

Training and empowering security professionals to build a trustworthy workforce

*Security training and education enables our national security by facilitating effective action among widely distributed, but connected, personnel and organizations as they combine their efforts to operate as a combined countermeasure to attacks against personnel, facilities and information desired by adversaries of the nation and its protected resources. By providing advanced training modules, enhanced curriculum and capability benchmarks, we enable our general workforce, security professionals and related constituencies to fulfill their responsibilities to their agencies and organizations who participate in the protection of the nation."*

**Kevin Jones**, Assistant Director, Security Training

The ST mission trains DOD, industry, DCSA agency security personnel and other government organizations to mitigate risk in support of national security. DCSA is the functional manager for security training for DOD, delivering security training and credentials to millions of members of the DOD trusted workforce annually.

DCSA's training efforts protect the nation by providing security training, education, certifications and credentials. These activities span a broad spectrum of security and counterintelligence disciplines, including credibility assessment, IS, PS, physical security, information security and insider threat.

Since the agency's stand up, ST has shifted from in-person training to a virtual and hybrid platform. While the move to more virtual training began in legacy DSS, COVID-19 restrictions forced the process to accelerate. In the past five years, ST has successfully brought together civilian and military security professionals from across the globe for the DCSA Security Conference for DOD, the DCSA Security Conference for Industry and the

inaugural Insider Threat Awareness Conference. As the pandemic waned, ST continued with key virtual courses while returning to in-person offerings, providing student flexibility and fulfilling demand. Annual course completions now stand at approximately five million.

ST also delivered over 9,000 proctored certification assessments to security professionals, enterprise-wide, through commercial testing at over 1,000 sites, worldwide. Over 6,200 Security Professional Education Development (SPeD) Certification conferrals were granted during this timeframe.





## On the Horizon:

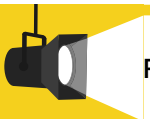
**DCSA Security Academy:** ST stood up the DCSA Security Academy in October 2024. This new schoolhouse is designed to centralize and refine training efforts across the agency. The Academy serves as a cornerstone for mission integration, emphasizing the creation of standardized, role-based learning pathways tailored to the needs of the security workforce. Other efforts include seeking accreditation to offer baccalaureate certificates and degree programs, transitioning to a new content management system (CMS) to improve ease of access and advancing certification programs.



### Did You Know?

The NCCA trains approximately 100 polygraph examiners each year for 30 partner agencies through a 12-week Psychophysiological Detection of Deception course. NCCA also provides continuing education for almost 1,000 federal polygraph examiners and conducts oversight inspections to meet its federal mandate.

DCSA provided operations security training in support of the National Defense Strategy when the SECDEF made the Operations Security (OPSEC) course and other courses in the CDSE catalog mandatory for all DOD employees. DCSA executed an OPSEC campaign comprised of four courses with an introductory SECDEF video which saw almost four million course completions. Through the infrastructure put in place to accommodate the OPSEC campaign, the following year DCSA was able to provide access to mandatory Controlled Unclassified Information (CUI) training to all DOD employees.



### REBECCA MORGAN ON THE STAND UP OF THE NEW DCSA SECURITY TRAINING ACADEMY

*"The new schoolhouse was established to ensure the mission readiness of America's Gatekeepers. Our learning audiences include DCSA FO and mission directorates with security responsibilities and other stakeholder audiences as directed. The DCSA Security Academy provides comprehensive mission training programs to develop the knowledge, skills and abilities required to support national security; tailored training programs to support mission readiness; and tools and resources to support mission integration across DCSA. Academy instructional staff are certified under Federal Law Enforcement Training Accreditation (FLETA) and/or DOD Policy Standards. Most of our staff have extensive experience in their respective fields having served as background investigators, IS representatives, adjudicators, or other mission roles. They marry deep subject matter expertise with advanced skills in instructional design and adult learning to bring high-quality training products and experiences to the DCSA workforce."*

**Rebecca Morgan**, Director, DCSA Security Training Academy





## Counterintelligence and Insider Threat

Preserving America's foundation of trust against foreign and insider threat

*Our success lies within our engagements and cooperation with other DCSA elements, the intelligence community, law enforcement, cybersecurity, National CI Task Force (NCTIF) and cleared industry. Each of these groups is vital in helping support the DCSA mission. Close relationships with other DCSA missions ensure that we can provide the necessary CI and insider threat support required to secure the trusted workforce."*

**Andrew Lochli**, Assistant Director, Counterintelligence and Insider Threat

The CI mission conducts activities to detect, understand and anticipate foreign and insider threats to the U.S. government's industrial base and workforce in support of the agency's IS and PS missions — both directly and through collaborative engagement with other intelligence community and law enforcement organizations. DCSA's CI functional services benefit from unique access to industry, building on its relationships across the industrial base. Since its inception, CI has worked diligently to encourage cleared companies to deter, detect and disrupt the theft of sensitive or classified U.S. information and technology by foreign entities.

Through our unique relationship and engagement with cleared industry, DCSA CI delivers threat information that educates and informs cleared personnel and cleared facility security programs. Industry, in accordance with 32 USC Part 117, reports Suspicious Contact Reports (SCRs) to DCSA

that identifies how foreign intelligence entities target the U.S. cleared national industrial base. On average, DCSA CI Special Agents (CISAs) conduct over 19,000 engagements with cleared facilities each year, delivering threat briefs, providing advice and assistance and supporting security reviews. Over the past five years, SCRs from industry grew from 29,126 in FY20 to 32,627 in FY24. This past year, those SCRs resulted in 2,824 Intelligence Information Reports (IIRs) shared with the intelligence community, and 714 referrals to other government agencies who took action and executed 161 investigations and operations. Through these collaborative efforts, cleared industry established effective CI programs that enhanced national security and promoted uncompromised delivery of sensitive and classified services and capabilities to DOD and other U.S. government agencies.

*The DOD Insider Threat Management and Analysis Center (DITMAC) plays a critical role in helping DOD's insider threat community to assess risk early in the process. The hope is that this early intervention stops people from actually becoming insider threats who pose an increased risk to other personnel, information, facilities and assets. These risks can also include things like workplace violence, domestic violence, suicide and espionage."*

**James Shappell**, Director, DOD Insider Threat Management and Analysis Center (DITMAC)

Reporting from cleared industry and academia results in DCSA's flagship product, the annual Targeting U.S. Technologies: An Assessment on Threats to Cleared Industry. This product — published at classified and unclassified levels — details potential foreign attempts to illicitly acquire U.S. technologies within cleared industry and identifies the most targeted technology categories and threat sources by geography.

The analytical support that CI successfully delivered to the NISP led to improved mission support to the unclassified DIB. Under DOD Instruction 5205.87 and in support of beneficial ownership, CI will expand its analytic capacity to include pre-award vetting of DOD contractors with contracts over \$5 million. This will enhance DCSA's threat visibility and ability to inform interagency partners, fostering a shared operating picture with the defense and intelligence communities.

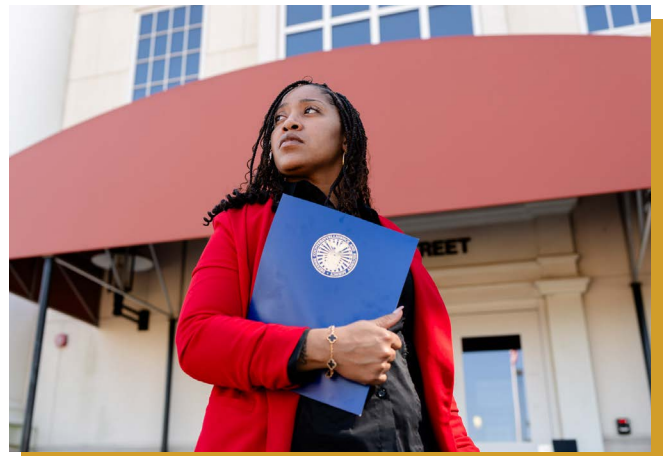
DCSA's activities and partnerships provide cleared industry and leaders within the federal government with a comprehensive threat picture. DCSA prioritizes constructive partnerships with cleared industry and academia to collectively mitigate theft of proprietary, sensitive or classified U.S. information and technology. These partnerships allow DCSA to effectively depict the overall national security threat picture to the cleared national industrial base.

Over the past five years, CI expanded and matured its role as a key conduit to the larger CI and law enforcement communities. The CI Partnership with Cleared Industry (CIPCI) program is a collaborative program designed by DCSA to promote CI information sharing. The CI Academic Outreach (CIAO) program facilitates and extends DCSA's collaboration to cleared universities in the NISP.

CI personnel provide classified and unclassified threat information related to their respective classified programs and personnel. These programs strengthen relationships and increase CI reporting. CI liaisons are deployed to federal and DOD agencies to further foster interagency cooperation and engagement.

DCSA synchronizes with national and DOD entities on intelligence collection requirements, production and community engagement with its placement of 56 CI personnel at local and national CI task forces. As a result, DCSA is increasingly recognized as a vital contributor to the national security enterprise.

Over the last two years, CI evolved the CI cyber program through the creation of eight cyber CISA positions across the field. Cyber CISAs are CI certified agents with cyber technical proficiency, specifically focused on addressing the growing CI threat in the cyber domain. They serve as specialized force multipliers, engaging with industry, integrating with DCSA field personnel and collaborating with the CI Cyber Mission Center (CMC). Their initiatives, integration and engagement with CMC, industry and partner agencies have already demonstrated value to the DCSA mission and increased cyber reporting.



## DC3 Collaboration

In 2019, DCSA and the DOD Cyber Crime Center (DC3) established a partnership to identify new strategies for sharing security information and data with the Defense Industrial Base Vulnerability Disclosure Program (DIB VDP) pilot. The DIB VDP was started in 2024. About 40 companies participated, providing information about their DOD-related networks and digital assets. Program officials and ethical hackers then searched for any vulnerabilities and helped remediate any issues. The pilot mostly focused on small to medium-sized companies. It is estimated that the pilot saved \$61 million, based on an estimated cost avoidance of \$4.3 million per breach.

DCSA also oversees DITMAC on the department's behalf. DCSA's Insider Threat functional services identify, assess and mitigate risks from insiders; oversee and manage unauthorized disclosures; and integrate, manage, mature and professionalize insider threat capabilities on behalf of DOD.

The DITMAC provides a centralized repository for insider threat information and coordinates with programs across DOD to ensure that all affected parties have the information they need to deter, detect and mitigate risks, closing critical information gaps.



In the past five years, insider threat incidences have attracted leadership attention, and DITMAC expanded its capabilities and services to meet the challenge. DITMAC modernization included:

- Incrementally improving the case management systems supporting insider threat reporting.
- Deploying insider threat advisors to the field to work with Commanders at 18 locations.
- Developing a contract to satisfy an existing gap in SIPRNet user activity monitoring analysis.
- Building the capability for an insider threat hotline that will be rolled out at scale in 2025.
- Expanding outreach to the DOD community through collaboration with the ST mission, including hosting an annual conference in collaboration with the OUSD (I&S).



DCSA also created the Behavioral Threat Analysis Center (BTAC) which is a centralized multidisciplinary team with the capability to contextualize and assess insider risk and recommend risk mitigation strategies for insider threats across the DOD enterprise.

### National Insider Threat Awareness Month (NITAM)

First observed in 2019, NITAM is an annual, month-long campaign during September that brings together thousands of U.S. security professionals and policy makers from government and industry, located in 25 countries around the globe, to educate government and industry about the risks posed by insider threats and the role of insider threat programs.



#### JOSEPH LAVILLE ON BUILDING RELATIONSHIPS WITH INDUSTRY ENGAGEMENT GROUP

*"I am fortunate to have had roles engaging with industry in the CI mission while at the Mid-Atlantic Region and headquarters. Whether in the field or at headquarters, our partnership and collaboration with cleared industry played a critical role in mitigating risks and ensuring a secure environment for the U.S. government and DIB. The CIPCI and CI CIAO are special partnerships that enable the U.S. government and industry to identify and articulate foreign intelligence threats, develop threat awareness briefs, and to share best practices with the entire DIB. For instance, CIPCI and CIAO partners shared their indicators and best practices for inclusion in DCSA's CI Best Practices for Cleared Industry booklet. Our industry partners have also been guest speakers at DCSA webinars to discuss current threats, such as the "Weaponization of Artificial Intelligence" webinar, which was attended by over 1,500 industry employees."*

**Joseph LaVille**, Chief, Counterintelligence Partnership Branch





## Evolution of Mission Support

Throughout its five-year history, DCSA expanded and matured its mission support capabilities to meet the demands of growing mission requirements and a dynamic operational environment.

The HCMO played a pivotal role in shaping the agency's workforce to meet the demands of its expanding mission. As DCSA stood up, HCMO prioritized transitioning over 3,000 employees to DCSA, ensuring payroll continuity and establishing a foundation for long-term workforce development. Since that time, HCMO's focus has evolved to develop a workforce model tailored to DCSA's unique requirements, while continuing to emphasize recruitment, retention and workforce planning.



### Did You Know?

In DCSA's inaugural year, 18 students were selected to be summer interns from an applicant pool of just over 100. By 2024, DCSA received 5,000 applicants with 75 students selected. The DCSA Student Experience program is a great feeder for new talent.

HCMO developed DCSA's first Strategic Workforce Plan (SWP) to guide critical workforce shaping activities to meet mission needs. It identified how the people and skill mix must change to achieve strategic outcomes by identifying competency gaps and priorities and mitigation strategies to address those gaps. The SWP guides DCSA's hiring priorities as the agency prepares for new mission requirements.

HCMO also made significant strides in building the professional development program by expanding the agency's Employee Leadership and Development Training and launching a Career Broadening Program to allow employees to work in different offices.

*The Career Broadening Program is an incredible opportunity that has deepened my appreciation of DCSA and has shown me how different components contribute to one greater mission."*

**Jillian Lien**, Special Agent, Virginia Beach Field Office, BI

DCSA's IT infrastructure transformation, led by the Office of the Chief Information Officer (OCIO), has been instrumental in modernizing its operational capabilities. The "DCSA One" initiative unified the agency's disparate legacy systems, creating a single, centralized IT environment. This effort standardized access to email, networks and critical resources, enabling employees to perform their roles seamlessly and securely.

DCSA is the first agency in the Department of Defense Information Network (DODIN) to successfully pass the Command Cyber Readiness Inspection (CCRI). CCRI increases the accountability and improves the overall security posture of the DODIN and is mandated by the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02D and Department of Defense Instruction (DODI) 8500.01, Cybersecurity.



## ROXANNE LANDREAU ON PROGRESS RELATED TO CYBERSECURITY

*“The DCSA CISO plays a vital role in protecting the agency’s information systems, personnel and mission. The CISO is responsible for maintaining a cybersecurity awareness and certification program, overseeing cybersecurity risks and ensuring DCSA systems and personnel are aligned with the Enterprise Security Operations Center (SOC). This enables the agency to respond to and disrupt potential adversary operations, while also conducting Cyber Defensive Operations to protect the DODIN. The CISO implements and enforces the RMF and oversees the Public Key Infrastructure (PKI) program, ensuring the secure issuance of certificates for authentication and encryption. By leading and coordinating the cybersecurity risk management posture, the CISO fosters a culture of threat awareness and resiliency, reducing internal and external attack vectors and safeguarding the agency’s information assets. Ultimately, the CISO’s efforts protect, secure and defend DCSA’s information systems, personnel and mission, while promoting a secure and resilient cybersecurity environment.”*

**Roxanne Landreaux**, Chief Information Security Officer



The Logistics Management Office transferred NBIS and CAS assets into a new, consolidated DCSA property book on day one of DCSA’s establishment. Assets and property value went from 10,217 assets valued at \$101 million to 20,086 assets valued at \$115 million.

Logistics Management also created a Master Space Plan to provide the agency with a comprehensive source of data and information on all 180+ DCSA facilities, including recommendations for facility consolidation and facility conditions. This allowed DCSA to prioritize resources to sustain and improve mission capabilities.

The preservation and usage of data across the agency has been central to its continued dedication to achieve efficiency and employ best practices. The DCSA Chief Digital and AI Office drove the effort to implement the DCSA data strategy to improve all DCSA mission and support area capabilities through adoption of enterprise data management practices and standards consistently.

The NBIS Data Integrated Product Team (NDIPT) was established to enable the successful data migration (selection, preparation, extraction, transformation, permanent movement and decommissioning) of appropriate data of the right quality, to the right place, at the right time without disruption to the PS mission.

The Office of the Chief Financial Officer (OCFO) seamlessly established a WCF at DCSA enabling the execution of EO 13869, which directed the transfer of the continuous investigation functional area from OPM to DCSA. Since that time, OCFO has embraced innovation and optimization in alignment with DCSA’s strategic priorities and DOD’s Financial Management Strategic Plan.



## MEREDITH MOORFIELD ON FM TRANSFORMATION INITIATIVES

*“The OFCO implemented a comprehensive transformation initiative to strengthen mission operations, both now and for the future. We’re advancing data accessibility for decision making, eliminating duplicative or error prone processes through automation and empowering our team to identify and own improvement initiatives. One of the most exciting parts of this effort is seeing day-to-day change, creating value for the agency and the taxpayer through gained efficiencies and informed decision-making.”*

**Meredith Morefield**, Chief of Staff, Office of the Chief Financial Officer



A key step to optimization was transition of the DOD continuous vetting and adjudications functional areas from a centralized appropriated funded program into the WCF, creating a financial end-to-end model for the entire PS mission, optimizing taxpayer dollars for services. This change promotes consistent operational and financial processing across the federal government through a unified service approach creating valuable insights with detailed financial reporting.

*“This change will promote consistent operational and financial processing across the federal government through a unified service approach. The WCF program will provide valuable insights with detailed financial reporting that can reduce our overall program costs.”*

**Jack Jibilian**, Chief, Financial Operations, Office of the Chief Financial Officer

Through a distinct innovation and transformation effort, the OCFO directed focus in adopting robotic process automation, machine learning and predictive analytics in all aspects of operations. Since the latter half of 2022, OCFO has developed more than 28 automations and saved more than 17,200 resource hours through automation of repetitive tasks, data transfers between systems and generating alerts for review and action. To emphasize the progress OCFO has made thus far, the fiscal year 2024 closeout harnessed automation to streamline the traditionally tedious process, completing key milestones three days ahead of schedule and slashing the workload by 40% over previous years.

The Contracting and Procurement Office (CPO) has grown and matured with the agency to become more responsive to agency demands while ensuring adherence to policy. CPO and the OCFO collaborated on the development and enhancement of the Acquisition and Budget Management (ABM) tool which took a once manual process for processing nearly \$1B in contract actions and automated it. CPO matured the agency Contracting Officer Representative program and improved the agency’s audit readiness while greatly enhancing contract oversight.

## Preparing for the Future Threat Landscape

The global security environment is rapidly changing. Our adversaries are employing increasingly sophisticated tactics to steal our technology, compromise our data and undermine our defense capabilities. These threats come in the form of cyberattacks, physical threats and even personal attacks on industry civilians. Today, the DIB spans a vast, global network of companies and supply chains. At the same time, the industrial base's expansive presence increases its exposure to risks and vulnerabilities.

Our adversaries are relentless in their pursuit of our intellectual property and technology. The rapidly increasing scale, scope and complexity of threats to our national security requires DCSA to be agile, integrated and aggressively innovative to meet the needs of the federal government and ensure our nation maintains its competitive advantage.

In early 2025, DCSA will publicly release an updated DCSA Strategic Plan – 2025-2030. The updated plan takes into account a threat environment that demands a potentially dramatic shift in the way DCSA operates. As the largest security agency in the federal government, the plan outlines three priorities that will allow DCSA to lead the security community in more efficient and innovative operations that elevate the ability to safeguard national security.

### Priority 1

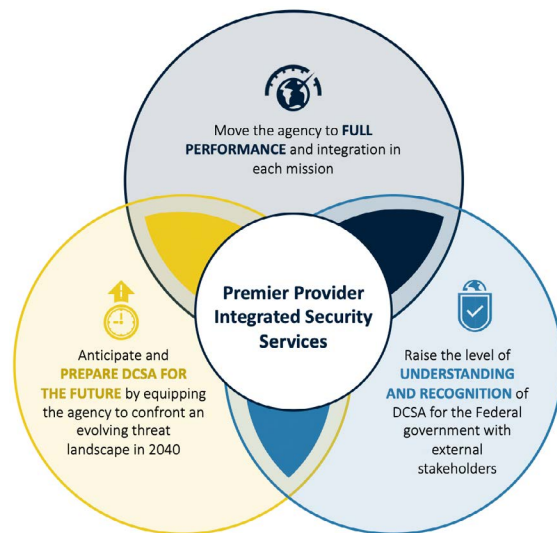
Move the agency to full performance and integration in each mission.

### Priority 2

Anticipate and prepare DCSA for the future by equipping the agency to confront an evolving threat landscape in 2040.

### Priority 3

Raise the understanding and recognition of DCSA as the premier provider of integrated security services for the federal government with external stakeholders.



These priorities are intended to help realize the full potential and power of DCSA and will be accomplished in the field and developed through collaboration between mission and field leadership. Along the way, in working together to achieve these goals, DCSA and its workforce will continue to challenge conventional thinking, and strive to deliver value to customers to enable national security outcomes, while embracing and embodying the agency's core values in all that it does — mission, people, service, integrity and innovation.



## Conclusion

DCSA has established itself as a cornerstone of national security, earning trust through its unwavering commitment to excellence. Over the past five years, DCSA has successfully addressed complex challenges by integrating legacy systems, expanding its capabilities and cultivating a workforce prepared to meet evolving demands. This foundation of trust has been built on a history of collaboration with industry, innovation and a steadfast dedication to protecting the nation's interests.

In the present, DCSA's maturation is evident in its robust mission support capabilities. From modernizing IT systems to streamlining personnel vetting processes, the agency has embraced cutting-edge solutions while maintaining continuity and reliability. These efforts ensure the integrity and security of operations, reinforcing trust among stakeholders, including federal agencies, cleared industry and the American people.

Looking to the future, DCSA remains committed to working with industry, DOD and partners across the federal government to advance the shared mission of protecting America's national security and the priorities set forth by DOD leadership. By adapting its capabilities to meet emerging threats, leveraging new technologies, reforming the acquisition process and strengthening the DIB, DCSA is proud to help uphold America's strategic military advantage and ensure that the U.S. military remains the strongest in the world.

The threats to our nation and industrial base are real, pervasive and ever evolving, and this agency and its partners must and will continue to adapt to meet these threats head-on. DCSA is well positioned to address tomorrow's challenges while safeguarding the principles of national security for generations to come.

This reflection on the past, acknowledgment of present successes and vision for the future underscores DCSA's enduring role as a trusted leader in both defense and security.

**DCSA: Safeguarding tomorrow, today.**

## Appendix: DCSA by the Numbers in FY24

### Personnel Security

**2.7 million+**

background investigations  
completed annually



**~4 million**

federal employees and  
contractors continuously vetted

### Industrial Security

**~13,000**

contractor facilities cleared for access  
to classified information under DCSA's  
security oversight responsibilities



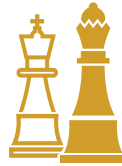
**~4,670**

IS reviews  
conducted annually

### Counterintelligence & Insider Threat

**4,600+**

insider threats  
processed annually



**32,600+**

suspicious contact reports  
received from industry annually

### Security Training

**~5.4 million**

security training courses  
completed



**~9,300**

certifications granted

### Field Operations

**174**

field locations



**2,200+**

field operators enabled

\*reflects FY24 data

## Appendix: History of Legacy Agencies

### Personnel Security Legacy

On December 29, 1971, the SECDEF established the Defense Investigative Service (DIS). This began the Department's unified handling of its personnel security, effective January 1, 1972.

In 1999, DIS underwent a reorganization to become DSS. DSS retained the personnel security investigation (PSI) mission until February 20, 2005, when the function was transferred to OPM.

OPM, as the successor to the Civil Service Commission, had been conducting PSIs for most non-DOD programs since 1953. That is when EO 10450 established the requirement for a government-wide PSI program and granted authority for the program to the Civil Service Commission. OPM became the government's largest ISP in 2005 after assuming the DSS program and personnel.

In May of 2012, the Deputy Secretary of Defense directed the establishment of the DOD CAF. The CAF would be comprised of the functions, resources and assets of the Army Central Clearance Facility, Department of Navy CAF, Air Force CAF, Joint Staff CAF, Washington Headquarters Services (WHS) CAF and Defense Industrial Security Clearance Office (DISCO).

In October 2016, the semi-autonomous NBIB was established under OPM. NBIB was the primary ISP for the federal government. It conducted ~95% of all federal background investigations.

On April 24, 2019, EO 13869 directed the transfer of NBIB from OPM to DOD, effective October 1, 2019.

### Industrial Security Legacy

In 1965, the Office of Industrial Security was established under the Defense Contract Administration Service (DCAS) and Defense Supply Agency (DSA). The change brought together more than 100 different offices of the Army, Navy and Air Force that had cognizance over plants handling defense contracts. In the reorganization, 11 CAS regions were established with uniform policies and regulations.

On Oct. 1, 1980, the ISP, the Key Asset Protection Program and the AA&E were transferred to the DIS from the Defense Logistics Agency (DLA). For 25 years (1980 until 2005) both the PS and IS missions were part of DIS/DSS.

The NISP was created in January 1993 by EO 12829. It was intended to replace not only the Defense Industrial Security Program (DISP), but the ISPs of the Central Intelligence Agency, the Department of Energy and the Nuclear Regulatory Commission.

## Appendix: Legacy History (cont.)

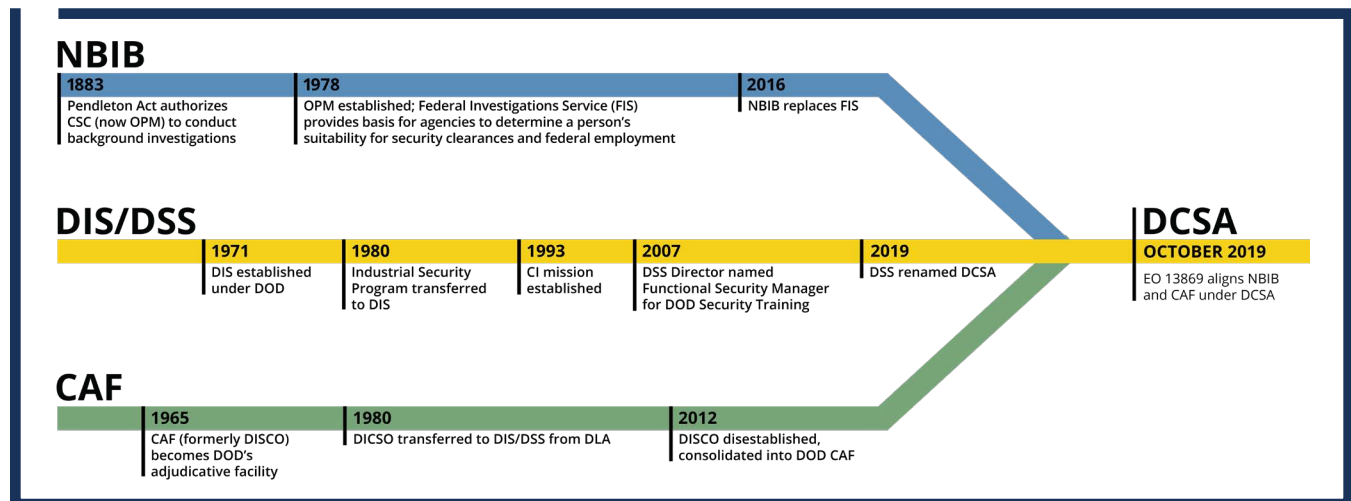
### Security Training and Education Legacy

The Department of Defense Security Institute (DODSI) was founded in 1972 under the DLA to train industrial security specialists and facility security officers. After the industrial security mission transferred from DLA to DIS, DODSI began training special agents to conduct PSIs. This training mission grew to include PS specialists and further expanded to include training for the military services and DOD agencies in the areas of information, personnel and physical security, adjudications and Special Access Programs.

On Jan. 1, 1984, DODSI was redesignated the Defense Security Institute (DSI) and in 1999, renamed to the DSS Academy. The Director of DSS was named the functional security manager for DOD ST in December 2007.

### Counterintelligence Legacy

The agency's Counterintelligence (CI) mission was established in May 1993. It established the DIS as responsible for: developing a CI employee awareness program; training CI investigators in a rapidly changing threat environment; reviewing subject interviews with CI relevance and extract significant information; serving as a clearing house for referrals of potential espionage cases to CI agencies for investigation; conducting internal inquiries into CI-related incidents and building an in-house CI program.





## Resources

1. Executive Order 10450, Eisenhower Administration, 1953.
2. National Industrial Security Program (NISP) Establishment, 1993.
3. Formation of the Defense Investigative Service (DIS), 1972.
4. National Defense Authorization Act (NDAA), 2016.
5. Executive Order 13869, President Trump, April 2019.
6. NBIB Operations Transfer to DCSA, October 2019.
7. DCSA Overview and Statistics, 2024.
8. Integration of CAF, NTC, and NCCA, 2020.
9. Transition of NBIS to DCSA from DISA, October 2020.
10. National Background Investigation Services (NBIS) Implementation.
11. Strategic Growth of DCSA, 2024.
12. DCSA Website: Comprehensive history, organizational details, and mission updates ([dcsa.mil](https://dcsa.mil)).
13. Gatekeeper Magazine: Official publication providing insights into DCSA operations and initiatives (Gatekeeper Magazine).

## Acronym List

<b>A&amp;A:</b> Assessment and Authorization	<b>CUI:</b> Controlled Unclassified Information
<b>AA&amp;E:</b> Arms, Ammunitions and Explosives	<b>CV:</b> Continuous Vetting
<b>AE:</b> Access Elsewhere	<b>DAU:</b> Defense Acquisition University
<b>AKC:</b> Applicant Knowledge Center	<b>DCAS:</b> Defense Contract Administration Service
<b>A&amp;S:</b> Acquisition and Sustainment	<b>DCSA:</b> Defense Counterintelligence and Security Agency
<b>AVS:</b> Adjudication and Vetting Services	<b>DC3:</b> DOD Cyber Crime Center
<b>BI:</b> Background Investigations	<b>DIA:</b> Defense Intelligence Agency
<b>BTAC:</b> Behavioral Threat Analysis Center	<b>DIB:</b> Defense Industrial Base
<b>CAE:</b> Component Acquisition Executive	<b>DIB VDP:</b> Defense Industrial Base Vulnerability Disclosure Program
<b>CAS:</b> Consolidated Adjudications Services	<b>DISA:</b> Defense Information Systems Agency
<b>CCRI:</b> Command Cyber Readiness Inspection	<b>DISCO:</b> Defense Industrial Security Clearance Office
<b>CDSE:</b> Center for Development of Security Excellence	<b>DITMAC:</b> DOD Insider Threat Management and Analysis Center
<b>CI:</b> Counterintelligence and Insider Threat	<b>DMDC:</b> Defense Manpower Data Center
<b>CIAO:</b> CI Academic Outreach	<b>DOD:</b> Department of Defense
<b>CIO:</b> Chief Information Officer	<b>DOD CAF:</b> Department of Defense Consolidated Adjudications Facility
<b>CIPCI:</b> CI Partnership with Cleared Industry	<b>DODI:</b> Department of Defense Instruction
<b>CISA:</b> CI Special Agent	<b>DODIN:</b> Department of Defense Information Network
<b>CISA(s):</b> CI Special Agent(s)	<b>DODSI:</b> Department of Defense Security Institute
<b>CISO:</b> Chief Information Security Officer	<b>DSA:</b> Defense Supply Agency
<b>CJCSI:</b> Chairman of the Joint Chiefs of Staff Instruction	<b>DSI:</b> Defense Security Institute
<b>CMC:</b> Cyber Mission Center	<b>DSS:</b> Defense Security Service
<b>CMS:</b> Content Management System	
<b>CORA:</b> Cyber Operational Readiness Assessment	

## Acronym List (cont.)

**e-APP:** Electronic Application

**EO:** Executive Order

**ESOM:** Enterprise SAFe Operating Model

**FO:** Field Operations

**FLETA:** Federal Law Enforcement Training Accreditation

**FOCI:** Foreign Ownership, Control or Influence

**HCMO:** Human Capital Management Office

**HISP:** High Impact Service Provider

**IIR:** Intelligence Information Report

**IS:** Industrial Security

**I&S:** Intel and Security

**ISP:** International and Special Programs

**ISP:** Investigative Service Provider

**IT:** Information Technology

**LACE:** Lean-Agile Center of Excellence

**LDP:** Leadership Development Program

**LE:** Law Enforcement

**NAESOC:** National Access Elsewhere Security Oversight Center

**NATO:** North Atlantic Treaty Organization

**NBIB:** National Background Investigations Bureau

**NBIS:** National Background Investigation Services

**NCCA:** National Center for Credibility Assessment

**NCITF:** National Counterintelligence Task Force

**NDAA:** National Defense Authorization Act

**NDIPT:** NBIS Data Integrated Product Team

**NISP:** National Industrial Security Program

**NISPPAC:** National Industrial Security Program Policy Advisory Committee

**NISPOM:** National Industrial Security Program Operating Manual

**NITAM:** National Insider Threat Awareness Month

**NSPT:** Non-Sensitive Public Trust

**NTC:** National Training Center

**OCFO:** Office of the Chief Financial Officer

**OCIO:** Office of the Chief Information Officer

**OMB:** Office of Management and Budget

**OPM:** Office of Personnel Management

**OpModel:** Operating Model

**OPSEC:** Operations Security

**OUSD:** Office of the Under Secretary of Defense

**PAC PMO:** Performance Accountability Council's Program Management Office

**PEO:** Program Executive Office

**PDUSD(I):** Principal Deputy Under Secretary of Defense for Intelligence

**PKI:** Public Key Infrastructure

**PS:** Personnel Security

**QART:** Quality Assessment Reporting Tool

**RMF:** Risk Management Framework

**SAFe:** Scaled Agile Framework

## Acronym List (cont.)

**SCI:** Sensitive Compartmented Information

**SCR:** Suspicious Contact Reports

**SECDEF:** Secretary of Defense

**SOC:** Security Operations Center

**SRP:** Security Review Proceedings

**SPeD:** Security Professional Education Development

**ST:** Security Training

**SWP:** Strategic Workforce Plan

**TW:** Trusted Workforce

**UoE:** Unity of Effort

**USD I&S:** Under Secretary of Defense for Intelligence and Security

**VRO:** Vetting Risk Operations

**WCF:** Working Capital Fund

**WHS:** Washington Headquarters Services





**Office of Communications and Congressional Affairs (OCCA)**

Russell-Knox Building  
27130 Telegraph Road  
Quantico, VA 22134

**Email**

[dcsa.quantico.dcsa-hq.mbx.pa@mail.mil](mailto:dcsa.quantico.dcsa-hq.mbx.pa@mail.mil)