

Official Magazine of the  
Defense Counterintelligence and Security Agency

# Gatekeeper



Volume 2, Issue 1



**TW 1.25  
milestone**

**TRANSFORMING LEGACY  
PERSONNEL VETTING PROCESS**

**ASK THE LEADERSHIP: LAURA EURY,  
FEDERAL INVESTIGATIVE  
RECORDS CENTER (FIRE)**

**IN THIS ISSUE**  
**EXCELLENCE IN CI AWARDS**

# IN THIS ISSUE

FROM THE DIRECTOR .....	3
DCSA, DOD AND GOVERNMENT LEADERS TRANSFORM U.S. PERSONNEL VETTING PROCESS VIA NEW TRUSTED WORKFORCE PROGRAM .....	4
ASK THE LEADERSHIP .....	8
INTRODUCING DCSA'S DATA STRATEGY: OPTIMIZING USE OF DATA TO IMPROVE MISSION AND BUSINESS EFFECTIVENESS .....	12
FIELD REORGANIZATION PART OF AGENCY'S TRANSFORMATION EFFORTS .....	16
DCSA ANNOUNCES WINNERS OF THE 2020 INDUSTRY AWARD FOR EXCELLENCE IN COUNTERINTELLIGENCE.....	19
DCSA EMPLOYEES RECEIVE COUNTERINTELLIGENCE AND SECURITY AWARDS .....	21
NEW RATING MODEL DESIGNED TO COUNTER THE THEFT OF CRITICAL PROGRAM AND TECHNOLOGIES .....	23
THE RIGHT QUESTION .....	26
BUILDING RELATIONSHIPS WITH KEY MANAGEMENT PERSONNEL (KMP) .....	29
REPORT INTERNATIONAL SECURITY VIOLATION IF LOSS, COMPROMISE OF FOREIGN GOVERNMENT INFORMATION..	30
ANNUAL FOCI CONFERENCE SPEAKERS FOCUS ON FUTURE, ADAPTING TO GREAT POWER COMPETITION .....	32
CONDITIONAL ELIGIBILITY DETERMINATIONS SAVE TIME, RESOURCES BY LEVERAGING USE OF CONTINUOUS VETTING TECHNOLOGIES .....	34
ADJUDICATIONS INCIDENT REPORT GUIDE FOR SECURITY MANAGERS .....	35
CUSTOMER ENGAGEMENTS TEAM PROVIDES CUSTOMER SERVICE SUPPORT FOR IT SYSTEMS .....	37

## Vol 2 | ISSUE 1

### DCSA Gatekeeper

Published by the Defense Counterintelligence and Security Agency (DCSA) Office of Communications and Congressional Affairs (OCCA)

### DCSA LEADERSHIP

William K. Lietzau  
**Director**

John Eskelsen  
**Chief, OCCA**

Cindy McGovern  
**Managing Editor**

Elizabeth Alber  
**Editor**

John J. Joyce  
**Staff Writer**

Christopher P. Gillis  
**Digital Content Specialist**

Tony Trigg  
**Layout, Editing and Design**

This Department of Defense (DOD) magazine is an authorized publication for members of DOD. Contents of the Gatekeeper Magazine are not necessarily the official views of, or endorsed by, the U.S government, DOD, or DCSA. The editorial content of this publication is the responsibility of OCCA.

All pictures are DOD photos, unless otherwise identified.

# FROM THE DIRECTOR



Happy New Year! This is the first Gatekeeper issue of what I am certain will be both a challenging and rewarding 2022. You may recall that a year ago we released the first issue of Gatekeeper with its new design and branding. And just over two years ago, we created a new agency. The women and men of DCSA have much with which to be proud, and our new flagship publication has done an admirable job in capturing the breadth of the new agency and the scope of its transformative changes.

DCSA's continued transformation is well-reflected in this issue. Our cover story regards DCSA's path to full implementation of Trusted Workforce 2.0 — the government-wide reform effort that will fundamentally transform the personnel vetting process. DCSA reached a significant milestone in that journey on Oct. 1, 2021, with the full enrollment of DOD as well as many other federal agencies in Trusted Workforce 1.25 (TW 1.25). Invented and implemented by DCSA in a mere year, TW 1.25 deferred the requirement for periodic reinvestigations by applying a risk-management approach to continuous vetting with carefully selected automated record checks. This new capability enables the early adoption of important TW 2.0 reforms and reflects what has truly been an all-of-DCSA effort. Although TW 1.25's significance is substantial, it is but one of many milestones in our trusted workforce journey. During 2022, DCSA will hit many more milestones as we both refine and expand the program to provide a more complete vetting picture.

Another article I want to highlight addresses another major milestone: Completion of the Agency's first Data Strategy. DCSA is a data-driven agency, and its establishment brought together myriad IT systems and databases designed to support unique needs that were not always optimal for the new, larger agency. In other cases, supporting systems were antiquated and unable to meet today's security standards. With our new Data Strategy, DCSA is undertaking a cultural shift toward a data-centric future using data to inform and guide how the agency plans, organizes and invests in new and innovative products and services. I believe this strategy will not only make it easier for the Agency to do its job, but it will permit us to deliver better and more informed products to our customers and stakeholders — thus enhancing security, both for the information itself, and for our nation.

The brief piece on the Security Review and Rating (SRR) Process for cleared facilities under DCSA cognizance touches a topic I know is a priority for our industry partners. Our review methodology has been in a state of flux that was exacerbated by COVID and our inability to conduct physical visits. We learned a lot from the early COVID-impeded virtual efforts, and I believe our industrial security team has developed a process that improves on past methodologies and captures a holistic reflection of facilities and their security programs. While we strive for consistency in oversight, each facility is unique, and this model allows for those differences while establishing a clear baseline compliance level.

Finally, this Gatekeeper issue presents our new regional structure and the attending geographic boundaries. The regional structure change helps to pull DCSA closer to full integration of our mission at the field level where the work of our customers and stakeholders takes place. Hopefully the regional changes are well-known to those whose points of contact have shifted.

DCSA is indeed an agency in transformation, and it is all for the good. America's Gatekeeper has never been more important. Thank you for reading and your continued support to DCSA.

A handwritten signature in black ink that reads "William K. Lietzau". The signature is fluid and cursive, with the first name being the most prominent.

William K. Lietzau  
Director,  
Defense Counterintelligence  
and Security Agency

# DCSA, DOD AND GOVERNMENT LEADERS TRANSFORM U.S. PERSONNEL VETTING PROCESS VIA NEW TRUSTED WORKFORCE PROGRAM

By John Joyce

Office of Communications and Congressional Affairs

The Defense Counterintelligence and Security Agency (DCSA) is implementing an ambitious plan to transform the nation's legacy personnel vetting process to ensure a trusted workforce throughout DOD, government and industry with a state-of-the-art system continuously vetting the nation's cleared national security population.

The plan requires a massive communications effort through the agency's internal and external media venues and social media platforms to publish press releases, news announcements and information updates apprising U.S. clearance holders and the public about the latest developments related to the reformed security clearance investigation process known as Trusted Workforce (TW) 2.0.

DCSA Director William Lietzau – in concert with senior leaders from the executive branch's Performance Accountability Council (PAC) – leads the effort to inform and explain the Trusted Workforce Program and its continuous vetting capability to military, government and contractor personnel at various events and symposiums in addition to briefings and interviews with broadcast, print and digital news media, including journalists representing trade and defense publications.

"Well before DCSA's stand up in 2019, U.S. policymakers worked to design a reformed personnel vetting policy based on a single secure vetting system for the country," Lietzau told reporters at a press briefing held at the Pentagon, Oct. 5, 2021. "The central component to that system is the continuous vetting of individuals in positions of trust who require a security clearance. That policy, called Trusted Workforce 2.0, is the culmination of a whole of government personnel reform effort that is overhauling the vetting process."

## Trusted Workforce 2.0

The TW 2.0 reform effort transforms the personnel vetting process and realigns it as one, government-wide system enhancing security while allowing reciprocity across organizations.

Moreover, the continuous vetting within TW 2.0 will fully replace periodic reinvestigations by employing a full suite of automated record checks, time and event-triggered activities, and analysis of agency-specific information through the National Background Investigative Services (NBIS). It fundamentally changes 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.

"We have been charged with implementing the Continuous Vetting Program and truly driving what that policy reform looks like," said Heather Green, DCSA assistant director, Vetting Risk Operations. "This includes our designs, plans and processes coupled with the secure information technology required to deliver that reform effort – specifically, continuous vetting. Our goal is to get ahead of potential insider threats through timely information sharing and mitigation actions."

The PAC — continuously advising DCSA on Trusted Workforce plans and policies – is comprised of the Director of National Intelligence as the security executive agent, the Office of Personnel Management director as the suitability and credentialing executive agent, the Undersecretary of Defense for Intelligence and Security, and the Office of Management and Budget's deputy director for management as principal members. Their guidance and collaboration with DCSA resulted in the risk-reducing phased approach of TW 1.25 and TW 1.5.

“Well before DCSA’s stand up in 2019, U.S. policymakers worked to design a reformed personnel vetting policy based on a single secure vetting system for the country”

~ Director Lietzau

“We are incredibly grateful to DCSA leadership for bringing us to where we are with Trusted Workforce 2.0,” said Matt Eanes, director of the PAC’s Program Management Office, which coordinates the government-wide TW 2.0 transformation. “There are over four million people enrolled in continuous vetting capabilities who won’t have to complete a periodic reinvestigation again. That could not have happened without DCSA’s implementation efforts. I don’t think anyone could have imagined a year ago that we would be here in 2021 with the DOD, government and industry national security sensitive population fully enrolled.”

### **Trusted Workforce 1.25**

DCSA accomplished the first step toward TW 2.0 in October 2021 by enrolling all of DOD and some federal agencies into an initial version of the Continuous Vetting Program via TW 1.25, which deferred the requirement for periodic reinvestigations by applying a risk-managed approach with select automated record checks.

Within a week of that step, Lietzau and Green held separate interviews with the media to announce the DOD full enrollment milestone while explaining how the TW 1.25 and TW 1.5 transitional phases will provide continuous vetting for all national security sensitive positions until the full TW 2.0 capability is ready in 2023.

“The speed to capability for Trusted Workforce 1.25 high-value automated record checks is a great example of a diverse group of folks within the agency coming together and focusing on a single mission-oriented goal,” said Program Executive Officer Terry Carpenter. “The acquisition program coordinated and collaborated with five or six agency offices leveraging existing technology for a secure operational capability that supported both DOD and federal components. This really demonstrates how agile IT system development can support meaningful

and incremental mission outcomes to reach Trusted Workforce 2.0 capabilities.”

The TW 1.25 capability enabled early adoption of important TW 2.0 reforms, particularly the continuous vetting of personnel with high-value data sources. The service performs continuous automated record checks against terrorism, criminal, and eligibility data sources on a daily basis. It also delivers alert management, real time threat analysis and reporting.

“Designing and implementing a new Trusted Workforce service in a short timeframe required coordinated effort across the agency,” said Juli MacDonald, senior advisor for Change Management and Strategic Planning in DCSA’s Chief Strategy Office. “Our Vetting Risk Operations and information technology folks worked hard to establish processes and solve every problem while the financial management team designed and initiated a new billing concept with procedures to make our vision become a reality on time.”

The financial management team’s communication to customers regarding the billing and price structure includes guidance about a new way they will pay for the Trusted Workforce service.

“The agencies will subscribe to a monthly service and have to know how to budget for it,” said Jack Jibilian, DCSA Working Capital Fund Operations chief. “There’s a lot of change management involved while working with our stakeholders to understand the new funding and billing methodology as we communicate the new way we’re doing business to our DOD, other federal agency, and industry customers. Although we are still analyzing our customer’s future costs for the full TW 1.5 service versus legacy background investigation products and services, they will certainly need to build their annual budgets much differently.”

**“Our team had to be transformed into an acquisition competency aligned organization in order to apply and focus resources towards the objective – transforming the personnel vetting mission via NBIS”**

~ Jeff Smith

Now that DOD and federal agencies are enrolled in TW 1.25, the next milestone is to work towards full enrollment in the second phase, TW 1.5.

“This is an incredible accomplishment and a major milestone for the national security community,” said Lietzau. “Not only does this allow us to help ensure the trustworthiness of the national security workforce, it helps identify and address factors that may lead to insider threat incidents, all while maximizing efficiencies across government. This is a major win for the security community.”

Lietzau – speaking about the progress and impact of the TW 1.25 and TW 1.5 phases to TW 2.0 – told the Defense Strategies Institute Counter Insider Threat Symposium on Oct. 20 that “we are on a good trajectory with Trusted Workforce 2.0,” adding that “it’s a major improvement of how we identify people and prevent potential threats.”

When DCSA receives an alert about a possible threat, the agency assesses whether the alert is valid and requires further investigation and adjudication. The continuous vetting system via TW 1.25 has issued a multitude of alert information to the DCSA team for investigation and validation years before clearance holders’ next periodic reinvestigation.

Lietzau cited recent examples where continuous vetting alerts enabled DCSA to take appropriate action. In one case, the system identified a security clearance holder under “an active investigation by another agency for potential terrorism activities, including a plan targeting United States facilities and ties to known or suspected terrorists.”

Lietzau recalled another case that involved an arrest warrant. Once alerted by the continuous vetting system about a federal employee accused of attempted murder and felonious assault, DCSA contacted law enforcement to confirm the individual’s identity and provided information that helped police apprehend the suspect.

## **Trusted Workforce 1.5**

Currently, select agency clearance holders are being enrolled into the automated TW 1.5 compliant capability that expands on TW 1.25 capability by continuously checking additional record sources comprising eligibility, terrorism, criminal activity, foreign travel, suspicious financial activity, credit bureau and public records.

TW 1.5 also features agency-specific records ranging from insider threat programs and security violation incidents to self-reported information and investigative work such as local law enforcement, employment conduct and subject interviews.

Meanwhile, the agency’s NBIS team is transforming the background investigation process to deliver stronger security, faster processing and better information sharing — replacing a suite of outdated, legacy IT systems.

## **NBIS**

“I have a team of heroes who figured out how to conduct design and development activities virtually during the pandemic,” said Jeff Smith, NBIS executive program manager, regarding the new personnel vetting information technology system’s development. “We positioned people in areas where they could develop, sanitize and promote the code adhering to cybersecurity best practices. Writing code at home can be done and dispersed in a virtual world but we had a responsibility to coordinate and make sure when we brought back in all the code – that it was integrated, cleansed and passed various cybersecurity checks to make sure it was production ready. From this position, we were then able to promote code into test environments to fully verify and validate NBIS functionality prior to deployment.”

NBIS and its advanced functionality to coordinate and connect the systems, interfaces and databases supporting continuous vetting, serves as a critical shared service enabling the future state TW 2.0 capabilities.

## BENEFITS OF TRUSTED WORKFORCE 2.0 AND CONTINUOUS VETTING

TW 2.0 is a bold, transformational approach that fundamentally changes the way the government establishes and maintains trust in the workforce. It shifts personnel vetting from evaluations every five to ten years to a continuous risk assessment model enabled by a new end-to-end suite of technology. It is designed to meet the dynamic needs of the 21st century in support of mission:

- Responsiveness to the mission will drive every aspect of personnel vetting. At its core, TW 2.0 reform is focused on delivering and maintaining a trusted workforce consisting of federal employees and contractors who are trusted to deliver on the mission, provide excellent service and demonstrate effective stewardship of taxpayer funds. Everything is accomplished through a mission-centric lens to deliver a trusted workforce to support the mission.
- The mobility of the trusted workforce is enabled as trusted individuals are available to support the mission where and when needed. This mobility unlocks the government's ability to deliver better services to the nation. It is accomplished by reducing complexity — removing friction from the process — to accelerate employee onboarding and knock down barriers to workforce movement between and within federal agencies and government contractors. Mobility is responsive to the mission, allowing individuals to move in and out of government seamlessly, driving innovation and making trusted individuals available to respond to agency priorities.
- Generating insight for decision-makers through earlier identification of indicators regarding behaviors of concern. This early awareness enables mission accomplishment by helping individuals who need assistance or by intervening in a situation when necessary. Continuous vetting in lieu of periodic reinvestigations, advancements in data analytics and improved information-sharing promote employee engagement before concerns evolve into more serious issues and enables decision-makers to make more timely and informed responses to potential threats.
- By helping individuals earlier, we keep trusted individuals on the job while removing those who might negatively impact the mission.

“Our team had to be transformed into an acquisition competency aligned organization in order to apply and focus resources towards the objective – transforming the personnel vetting mission via NBIS,” said Smith. “We, DCSA have actually developed our own acquisition command within the agency to develop and manage acquisition programs such as NBIS. This is a unique construct — to have an acquisition command placed within an operational command to meet mission objectives.”

Smith and his team are planning and deploying iterative NBIS capability deployment that involves onboarding and adoption in a phased approach. This gradual rollout is designed to ensure NBIS capabilities have gone through significant government and user acceptance testing while DCSA fine-tunes the onboarding process for the best customer experience.

“The DCSA team’s dedication and hard work to overcome obstacles enabled personnel security reform efforts via continuous vetting to become a reality for the federal enterprise,” said Green. “The team met our challenging continuous vetting enrollment goals while developing a new capability to identify derogatory information earlier than the traditional periodic reinvestigation. I’m very proud of their accomplishments to grow and build a very robust vetting program that will protect national security.”

**“The DCSA team’s dedication and hard work to overcome obstacles enabled personnel security reform efforts via continuous vetting to become a reality for the federal enterprise”**

~ Heather Green

# ASK THE LEADERSHIP



*By Laura Eury*

*Deputy Assistant Director for Federal Investigative Records Enterprise (FIRE)*

*Editor's Note: In each issue of the Gatekeeper, we feature an interview with a senior leader on their background, mission and program priorities.*



**Laura Eury, Deputy Assistant Director for FIRE**

Laura Eury serves as the Deputy Assistant Director for Federal Investigative Records Enterprise (FIRE). FIRE supports the government-wide Background Investigations (BI) mission.

Eury leads a workforce of close to 1,000 federal and contract staff, spread across multiple states who are responsible for the processing, automation, and management of government-wide investigative records collection and analysis, and end-to-end case processing functions. This includes the scheduling of 2.4 million investigations per year, operating the ingest and delivery of investigations to customer agencies, conducting automated record checks, and establishing relationships and agreements with both Federal, state, local, and commercial data brokers.

Prior to this position, Eury was the Executive Program Manager for BI field contracts, where she led a team focused on the development of program requirements, technical administration, and oversight of over \$2 billion in contracts.

Eury joined the Office of Personnel Management (OPM)'s Federal Investigative Services in 2006. As the Assistant Director for Management Services her team provided a broad range of services including the Executive Branch Suitability Adjudications program and management of Contracting Officer Representatives for investigative contracts worth over \$3 billion.



# QUESTIONS AND ANSWERS

## **Please tell us about your background. How did you end up in FIRE?**

I started my Federal career in 2003 with the Naval Audit Service as an auditor, where I performed operational audits on major Navy weapons system acquisition programs. I joined the Office of Personnel Management Federal Investigative Services in 2006. I've held various roles throughout my tenure in this mission space which has given me a wide range of experience in many facets of the investigations program. I served as the Program Manager for the Freedom of Information and Privacy Act office where I was responsible for establishing and overseeing the protection, retention, and disclosure policies of investigative files and processing the release of agency records. I served as the Assistant Director for Management Services leading a team that provided a broad range of services including the Executive Branch Suitability Adjudications program and management of the Contracting Officer Representatives for the major investigative contracts worth over \$3 billion. Prior to my role in FIRE, I served as the Executive Program Manager for BI field contracts where I led a team focused on the development of program requirements, technical administration, and oversight of over \$2 billion in contracts. These contracts provided a contractor workforce of over 3,000 background investigators for national security and public trust purposes. All of these experiences have prepared me well to be part of the FIRE team.

## **What is FIRE?**

FIRE is the Federal Investigative Records Enterprise, which is a component in the Background Investigations (BI) mission. We are responsible for the processing, automation, and management of government-wide investigative records collection and analysis, and end-to-end case processing functions for the BI mission.

## **How does FIRE support the agency's mission?**

FIRE is a critical operational component of the BI mission that supports the delivery of high-quality, timely, and relevant investigative services to secure the trustworthiness of the U.S. government's workforce. FIRE handles the scheduling of 2.4 million investigations per year and the collection of over 17 million records through automated and human review methods. We also have established relationships and have executed over 100 investigative record agreements with both Federal, state, local, and commercial data brokers in order to obtain the investigative records needed to meet the Federal Investigative Standards.

## **How did it start?**

FIRE was officially formed in 2016 during a reorganization of the BI mission. It was formed by merging operational, contract oversight, and records outreach and analysis components all under one umbrella since there were clearly synergies. The intent was to better align these business processes to support the investigation record collection and processing functions. The Operations and Outreach centers were created within FIRE that work together to deliver upon our mission. Each FIRE center relies on the other to perform their job. The Outreach center ensures that the relationships, agreements, and connections are in place to collect the investigative records and the Operations center processes the cases and records. Communication and partnership is key in FIRE.

## **Why did the BI mission need an organization like FIRE?**

Previously, BI was organized by like functions meaning that all contract oversight was in one division regardless of the business process it supported. In order to create agility and enhance our business process transformation efforts, we decided to align with an eye towards business processes. This allowed organizations to take better ownership over their business processes to make real-time enhancements and ensure their business processes supported the other BI elements' needs.

---

## How many people work for FIRE? What do they do?

---

We are an organization of 131 Federal employees and over 700 contractor staff. Our federal staff have diverse responsibilities to ensure the FIRE processes are continuously optimized to assist in the delivery of investigative services. We have staff that oversee the financial aspects of our investigative record agreements, work with record providers to obtain or improve the collection of investigative records, perform record collection and record review, provide contract oversight, and focus on process improvement and robotic process automation tools. We have a wide-breadth of expertise in our staff that enable the FIRE mission to continuously evolve and improve to support the BI mission.

---

## How has FIRE developed over time?

---

FIRE excels in evolving with changes in technology, policy, and environment. At one time, many of the FIRE responsibilities involved a person processing hardcopy material. Over the years, and especially as a necessity with COVID, automated tools have been incorporated into the workflow, which has completely eliminated the need for a hardcopy case file. These developments have allowed FIRE to reallocate resources to improve other areas of the mission. FIRE is constantly seeking new methods for obtaining records, processing work, and improving the timeliness and quality of the overall background investigation.

---

## What have been the most significant changes for FIRE since its creation?

---

FIRE has had the unique opportunity to incorporate different types of technology into the processes that we use to request, obtain, and review information. These different types of technology include the use of the Robotic Process Automation. In addition, when FIRE was originally created, most data providers maintained hardcopy records and obtaining records was a very manual and time-intensive process. Since then, data providers have made significant strides in automating their records and making them available electronically. Further, as a result of COVID, many of our operations that were previously performed onsite in Boyers, Pa., have been adjusted and can be performed remotely. I am proud of the advancements we have made and the ability for us to maintain the mission during this challenging time.



---

## What are the biggest challenges facing FIRE?

---

I think the biggest challenge for FIRE is the pace of change. We work in an environment that has evolving threats, increasing technology and capabilities, and changing environments for our record providers that impacts how they support us. We also have new investigative policies and a new IT system on the horizon that we will need to plan for and implement. This creates a challenge for us to ensure we keep the mission working efficiently and effectively today through whatever challenges arise to meet the quality and timeliness needs for our customers. If we have one day of an IT outage within DCSA or with our record providers it likely impacts thousands of investigations. So while we keep our eye on today, we have to plan strategically for the future to ensure our mission and workforce are ready for the transformation journey.

---

## What are the opportunities and where is FIRE going in the future?

---

I know I have focused on how FIRE supports the BI mission; we are a critical piece in enabling the BI mission's performance and the need for the work that FIRE performs will not change. However, the way we perform the work will surely change as the Personnel Vetting enterprise, DCSA, and BI transforms to meet new investigative standards through Trusted Workforce 2.0 and implements new technologies in the National Background Investigation Services. I have to mention how FIRE helps the larger Personnel Vetting Enterprise throughout the government. Many other agencies utilize our expertise, relationships, and connections to deliver on their investigative missions. As the enterprise continues to encourage shared services with an eye on building once and using many, we anticipate the need for the FIRE work to be ever more important for the community. It is truly exciting to be part of this journey in ensuring a Trusted Workforce!



# INTRODUCING DCSA'S DATA STRATEGY: OPTIMIZING USE OF DATA TO IMPROVE MISSION AND BUSINESS EFFECTIVENESS

By Wallace "Wally" Coggins

Chief Data Officer (CDO) and Acting Chief Strategy Officer (CSO)

On Sept. 13, 2021, DCSA Director William K. Lietzau signed the agency's first Data Strategy — an important milestone in DCSA's transformation journey. When the agency was created, it brought together different data management methodologies, and numerous incompatible databases and systems supporting different mission and support areas, requiring the agency to define more stringent security requirements and controls for ethical data sharing and use. With this new Data Strategy, DCSA is enabling an agency-wide cultural shift toward a data-centric future; purposefully leveraging knowledge of its data assets to shape how the agency plans, organizes and invests in new and innovative data products and services. As DCSA continues to integrate critical support programs, and the personnel security, industrial security, and threat detection and mitigation missions, we need a unified approach to managing our data.

## TRANSFORMING DATA MANAGEMENT TOGETHER

The Chief Strategy Office developed the DCSA Data Strategy through a deliberate dialogue with the whole enterprise, ensuring every agency organization contributed to its development. This close collaboration was critical in developing a unified vision and approach, while simultaneously assessing and fostering workforce data literacy and maturity. DCSA's collective approach to managing data will ensure mission and support areas are positioned to find, use, and share data as mission dictates and data management will remain central to providing more reliable services to our customers and more comprehensively ensuring the trust of cleared facilities, systems, and personnel.

### Data-centric vs. Data-driven

At DCSA, data lies at the heart of agency operations. The DCSA Data Strategy is about transforming a highly sophisticated data-driven enterprise into a data-centric one.

**Data-driven** means an organization relies on data to make decisions, and the organizational focus is on building technology tools and applications, capabilities, and a culture that acts on data.

**Data-centric** means an organization values its data as a strategic and enduring asset, purposefully cared for throughout its life. Data-centric organizations realize that data is the only constant in an ever-changing world. The data-centric approach requires a data strategy that is technology-agnostic with an ability to be flexible and adaptable to leverage new technologies within a timeless governance framework.

# “DCSA is enabling an agency-wide cultural shift toward a data-centric future”

## DCSA'S Data Strategy Framework

The DCSA Data Strategy Framework, consistent with the DOD Data Strategy of 2020, establishes a Vision, Guiding Principles, Essential Capabilities and Goals.



### Vision Statement:

Trusted data at speed and scale empowering America's gatekeepers to protect our nation's critical assets.

### Guiding Principles:

The guiding principles reflect the agency's philosophy and core values upon which the data-centric future is built. It is vital that the agency acquire, use and share data with a solid foundation of ethical responsibility, protecting privacy and civil liberties of citizens, with whose data it has been entrusted.

### Essential Capabilities:

**Data Architecture** -- achieve effective enterprise change by mapping strategy and business requirements to data assets, informing technology investments.

**Data Standards** -- make it easier to create, share, and integrate data by providing a clear understanding of how the data is represented, and that the data received is at the level of quality expected.

**Data Governance** -- ensure proper oversight required to effectively manage and invest in data assets to achieve business value.

**Workforce Talent and Culture** -- continually enhance the ability to understand and use data to make evidence-based decisions and transform the enterprise toward a data-centric future.

## Goals:

---

DCSA leverages and expands upon the DOD goals, with measurable objectives tailored to meet the unique needs of the agency:

**Visible** – We can locate the data we need.

**Accessible** – We can retrieve the data we need.

**Understandable** – We can recognize the content, context, and applicability of the data we need.

**Linked** – We can utilize data elements through innate relationships.

**Trustworthy** – We can be confident in all aspects of data for decision-making.

**Interoperable** – We have a common representation/comprehension of data.

**Secure** – We know that data is protected from unauthorized use and manipulation.

Each of these goals carry multiple objectives to ensure DCSA is making progress. For example, to ensure data is “Visible”, the objective is to make agency data sources and information sharing agreements accounted for in an Enterprise Data Catalog; a centralized listing of the data and its characteristics. To ensure data remains “Secure”, DCSA will establish strict data security processes and protocols to govern the access to, use of, and disposition of data.

## IMPLEMENTING THE DCSA DATA STRATEGY

---

DCSA will implement the Data Strategy in two phases. Phase one establishes the framework and high-level notional roadmap to guide engagement with the workforce. Phase two continues the roadmap evolution by integrating findings from the Data Maturity Assessment efforts, identifying resource commitments, and prioritizing efforts in alignment with agency strategic priorities.

The DCSA Enterprise Data Management (EDM) Program laid the foundational work to implement the strategy and has already seen successes:

### DCSA’s Data Maturity Assessment (DMA): Permanent Self-Assessments

---

Before DCSA could execute the Data Strategy, it needed to understand the level of data maturity, and tailor enhancements to mission and support areas’ specific needs. To do that, DCSA conducted a Data Maturity Assessment (DMA) using industry leading models. This assessment is ongoing and will be conducted on an annual basis to monitor the program. Initial feedback shows 92% of surveyed government employees believe that data literacy is critical to their missions, indicating readiness for change.

### Collective Data Governance: The Data Stewards Council (DSC)

---

On October 23, 2020, DCSA established the DSC, a decision-making body overseeing the agency-wide stewardship of DCSA data assets. The DSC is the agency’s first formal data governance body, and is comprised entirely of designated members from the DCSA workforce.

Council members, known as Data Stewards, ensure strategic data assets are safeguarded appropriately and made available to authorized personnel and mission partners in compliance with applicable laws, regulations, and policies. This body also lends the critical voice of the business unit level, influencing more positive mission

outcomes, and the delivery of more reliable agency services to our customers. The DSC also functions to activate the Essential Capabilities.

## Using Our Data: Data Agreements and Cataloging

---

The DCSA CDO is refining the agency's processes for data sharing agreements to improve interoperability, as the agreements outline the parameters for sharing data between the agency and its Federal and DOD mission partners and its customers. Data agreements are critical for ensuring DCSA data is shared securely and in accordance with the authorities under which it is collected.

Simultaneously, the DCSA CDO is establishing an enterprise data catalog, which is the hub for knowledge sharing and information exchange about data assets, and their relationship and impact upon all levels of the enterprise. A data catalog is a collection of information about the agency's data assets that helps analysts and other data users to find the data that they need, serves as an inventory of available data, and provides information to evaluate suitability of data for intended uses. The data catalog is an enterprise governance capability essential to understanding the impacts of data on agency strategy, business operations, and technology, driving agency transformation and modernization, improving interoperability and information sharing, while implementing privacy, ethical data use, and security by design. The agency's data catalog efforts will integrate into the DOD federated data catalog in accordance with DOD policy.

## EMPOWERING DCSA FOR THE FUTURE

---

Implementing the Data Strategy ultimately makes it easier for the agency to do its job, and harder for adversaries to undermine national security. By exercising command over our data and securing it appropriately, we can ensure it exclusively supports the DCSA mission and that of our partners.

# FIELD REORGANIZATION PART OF AGENCY'S TRANSFORMATION EFFORTS

*By Juli MacDonald  
Chief Strategy Office*

The Defense Counterintelligence and Security Agency (DCSA) executes its primary missions through an extensive network of background investigators, industrial security representatives, information system security professionals, and counterintelligence (CI) special agents located across the United States. The majority of DCSA's workforce operates in the field and works daily with customers, industry partners, and stakeholders. For this reason, field transformation is a critical component of DCSA's Operating Model (OpModel), which is guiding the broader DCSA transformation journey to operate more effectively and efficiently as the nation's Gatekeepers.

DCSA was formed through the merger of numerous security organizations — Defense Security Service (DSS), DoD Consolidated Adjudications Facility (CAF), and National Background Investigations Bureau (NBIB) — inheriting legacy structures and siloed operations for their respective field workforces. Each organization had its own structure to manage its field operations. Legacy NBIB included three regions, while legacy DSS was divided into four. To build a unified field structure, the Chief Strategy Office (CSO) worked closely with mission leaders across the Background Investigations (BI), Critical Technology Protection (CTP), and Counterintelligence (CI) mission areas.

This transformation is being implemented through a phased approach focused on realigning regional boundaries, determining new regional headquarters locations, and building a cohesive organizational structure — all with a focus on making fieldwork processes far more efficient and effective.

## NEW REGIONAL FIELD STRUCTURE

The first phase of DCSA field transformation was creating regional boundaries that unified the legacy field structures into one DCSA structure for the BI, CTP, and CI missions. The new structure merged seven regions into four: Western, Central, Eastern, and Mid-Atlantic. The new regional structure took effect on Oct. 1, 2021.

A cross-functional team, including representatives from each mission area, analyzed workforce data from across the field to create this new structure that balances the workload across the four regions. With the new boundaries, some stakeholders were assigned new DCSA points of contact. CI special agents, industrial security representatives, or information systems security professionals have contacted affected stakeholders and to ensure there is no break in mission operations as the agency implements the new structure.

## NEW REGIONAL FIELD HEADQUARTERS LOCATIONS

The second phase of transformation was to identify new regional headquarters in each region. To determine the best locations to support mission execution, the team conducted an objective analysis, using four criteria:

- Access to secure systems and networks necessary for mission execution;
- Distance and travel time to field offices, cleared facilities and industry partners, and access to a major airport/airline hub;
- Facility and space requirements to allow for near and long-term occupation, including availability of classified and non-classified space; and
- Alignment to the agency's strategic plan

The DCSA director announced the new headquarter locations in early October during an agency town hall. The regional headquarters include: Andover, Massachusetts for the Eastern Region; Alexandria, Virginia for the Mid-Atlantic Region; Farmers Branch, Texas for the Central Region; and Southern California for the Western region. The exact location in Southern California has not yet been determined and requires additional analysis on feasible facility options.

The process of standing up the new headquarter locations and offices will take time and will begin to take shape as the new regional leadership positions described below are filled. The vision is to have a regional support staff operating out of the headquarters locations to help drive a unity of effort across each region.

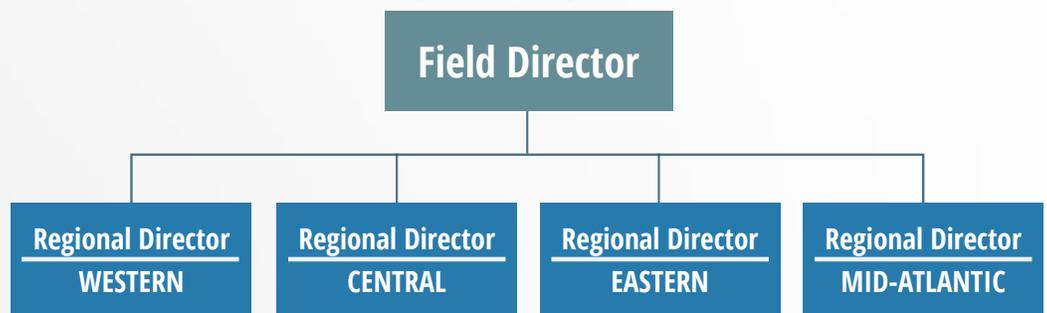


## REORGANIZING DCSA'S FIELD LEADERSHIP STRUCTURE

The third phase of field transformation is to establish a new field leadership structure to promote mission coordination, and policy and process alignment. Creating consistent organizational structures across the regions will empower the field workforce to share information and collaborate across both missions and regions.

The new structure includes new positions to help lead the field workforce and be responsible for key administrative, logistical, and cross-mission coordination functions. The Field Director is a new position responsible for ensuring standard operations and resources across the field. This person will be the voice of the field at DCSA headquarters, ensuring that issues facing the field workforce and the stakeholders they serve will be top of mind for agency leaders. Regional Directors, another new position, will oversee administrative, logistics, and cross-mission information sharing for the region. This position is also responsible for helping ensure consistent execution of policies/procedures across missions and regions.

These new positions will allow more time for the current regional leaders to focus on mission execution, by relieving them of administrative and logistical responsibilities for their field workforces.



In addition to promoting consistency and efficiency for the workforce, this new structure will bring more leadership closer to industry partners and other stakeholders with an aim to increase communications and engagement to improve mission outcomes.

In fiscal year 2022, DCSA will focus on hiring the new Field Director and the four new Regional Directors. As the agency hires these new positions, it will be designing and building the regional support teams and processes to support further regional integration. This new regional organizational structure will create unity of efforts in the field and promote a common culture shared by each DCSA mission area.



## THE IMPORTANCE OF BRINGING THE FIELD TOGETHER

---

Field integration is not an end goal in itself, but is a means to the end of optimizing mission performance. Unity of command within the field will inform the consistent application of policies related to space, vehicles, supplies, information technology (IT), and more general resourcing across the missions. An example of this is a recent effort to migrate all missions to one IT network, which supports information sharing across the agency. Beyond this however, field alignment will yield improved performance through coordination across missions. The intent is to design processes, data strategies, and technologies that enable more timely information sharing as well as identify what is currently hindering integration.

Integration will lead to increased information sharing, which will help DCSA create a shared situational awareness of risks. To facilitate this, the agency is developing a new Security Risk Management Capability to provide a more holistic view of vulnerabilities, threat, and consequence information across the agency through enhanced analytics and case management abilities. This effort is focused on identifying and building out exactly how DCSA will share information about risks, to include supporting policies, procedures, and resources. While this is a significant undertaking that will take time to come to fruition, it will further support a culture in which the workforce is acting together to be more effective Gatekeepers.

By creating unity of command in the field through a new regional field structure, headquarters' locations, and organizational structure, DCSA is laying a strong foundation to transform how DCSA operates as an agency. Unity of command will lead to new ways of working together as Gatekeepers.



# DCSA ANNOUNCES WINNERS OF THE INDUSTRY AWARD FOR EXCELLENCE IN COUNTERINTELLIGENCE

Four cleared facilities earned the FY20 Defense Counterintelligence Agency (DCSA) Excellence in Counterintelligence (CI) Award. DCSA annually recognizes those cleared companies that exhibit the most impressive CI capabilities and cooperation with U.S. Government efforts to deter, detect, and disrupt the theft of sensitive or classified U.S. information and technology by foreign entities.

The Excellence in CI award is intended to encourage highly mature and effective CI programs that enhance national security and promote the uncompromised delivery of sensitive and classified services and capabilities to the Department of Defense (DOD) and other U.S. Government agencies.

Candidates for this award are identified by DCSA field personnel and formally nominated by a panel consisting of the DCSA regional CI directors. After the nominations arrive at DCSA headquarters, a panel composed of senior leaders from across the DCSA enterprise conducts a multi-stage selection process to identify annual winners based on the assessment of CI/Insider Threat Reports the company submitted that specifically led to the opening of full field investigations, operations, or other activities by federal agencies. Other significant company actions that detected and countered foreign intelligence activities are also considered, including actions that led to disruptions, prosecutions, convictions, debarments, and administrative actions.

## The following highlights each winner's fiscal year 2020 efforts and how they achieved excellence in counterintelligence.

### **BOOZ ALLEN HAMILTON INC.**

Booz Allen Hamilton Inc., headquartered in McLean, Va., is one of the largest cleared contractors supporting the U.S. government. Booz Allen executes an advanced corporate level CI and Insider Risk Management Program leveraging the latest technology and methods to identify and investigate threat indicators.

Booz Allen's suspicious contact reporting (SCR) resulted in the dissemination of CI Reports (CIR) and referrals to multiple Federal CI and Intelligence Community (IC) agencies. The majority of Booz Allen reports also met national level collection requirements and were published and disseminated to the IC as Intelligence Information Reports (IIR), drawing separate interest from the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), the Air Force Office of Special Investigations (AFOSI) and the National Aeronautic and Space Administration (NASA).



## THE GEORGIA INSTITUTE OF TECHNOLOGY

The Georgia Institute of Technology (Georgia Tech)—based in Atlanta, Ga., and inclusive of its 13 geographically separated cleared field locations—runs a highly mature and comprehensive CI and Insider Threat program while managing strong partnerships with Cyber Security and Export Control programs. The program exceeds that of most cleared contractors of similar size and complexity, as well as within academia. Georgia Tech's program and personnel have identified and thwarted a broad range of foreign threats; such as, undisclosed participation in foreign talent programs, improper activities by foreign scholars, and cyber-attacks.

Georgia Tech reporting to DCSA resulted in one operation involving other government agencies; one full field investigation involving three subjects and two disruptions of foreign efforts against sponsored microelectronic research, as well as unilaterally identifying an early threat to Operation Warp Speed, a partnership between the Department of Health and Human Services (HHS) and DOD, aimed to help accelerate the development of a COVID-19 vaccine. Additionally, the majority of Georgia Tech FY20 reports met national level collection requirements and were published and disseminated to the IC as IIRs, where positive evaluations were received.



## THE MITRE CORPORATION

The MITRE Corporation (MITRE), headquartered in McLean, Va., operates six federally funded research and development centers (FFRDCs), government-sponsored entities that support a federal agency's mission with long-term research and development, including enhancing organizations' CI/cybersecurity assurance. For example, MITRE provided direct support to Operation Warp Speed to prevent foreign adversaries from disrupting or stealing domestic COVID-19 research.



In support of the FFRDCs special relationship with the government, MITRE maintains a corporate CI program that employs unique and proprietary tools and techniques to defend itself against persistent CI threats. MITRE detected and reported 84 SCRs/CIRs to DCSA, resulting in DCSA referrals to the FBI, the Defense Criminal Investigative Service, and other government agencies. In FY20, one MITRE report to DCSA resulted in immediate FBI response to mitigate a specific threat; other MITRE reporting resulted in 34 IIRs directly responsive to national collection requirements.

## PURDUE UNIVERSITY

Purdue University, located in West Lafayette, Ind., maintains a robust CI program grounded in close collaboration with DCSA and the FBI, and the establishment of strong policies to protect research from foreign influence. All cleared Purdue personnel and those who work on controlled unclassified information (CUI) projects receive training regarding potential conflict of commitments and reportable outside activity making clear that all outside and international activity is reportable.

Purdue University's reporting in FY20 resulted in 18 CIRs referred to Federal Agencies and 48 IIRs responsive to national collection requirements. Reporting from Purdue University substantially supported a major investigation involving NASA and FBI offices in Indianapolis, Ind.; Springfield, Ill.; St Louis Mo.; and Buffalo, N.Y. Other Purdue University reporting resulted in at least two operations by a task force comprised of several U.S. government agencies. Separately, Purdue University disrupted efforts by foreign-backed companies from trying to gain access to research partnerships at Purdue.



# DCSA EMPLOYEES RECEIVE COUNTERINTELLIGENCE AND SECURITY AWARDS

Employees of the Defense Counterintelligence and Security Agency received recognition in three categories of the 2021 Intelligence Community National Counterintelligence and Security Center (NCSC) Professional Awards. The NCSC recognizes individuals and teams across the Intelligence Community (IC) who made significant contributions to CI and security missions during the previous calendar year.

**There are 12 categories for which nominations can be made, and this year, two individuals and one team from DCSA won awards:**

## **Industrial Security - Individual:**

Ann Marie Smith  
(San Francisco Field Office, Western Region/Operation Warp Speed)

## **Education/Training - Individual:**

Edwin Kobeski Jr.  
(Center for Development of Security Excellence)

## **Education/Training - Team:**

Insider Threat Division (CDSE)

**S**mith, a senior industrial security representative, is recognized for significant contributions in applying her security experience to Operation Warp Speed (OWS). Her technical skills, decades of experience, and personal contacts came together to establish new techniques that contributed to reducing risk, protecting the supply chain, and ensuring the uncompromised delivery of multiple product lines. OWS is the nationwide, all-of-government effort with the goal of delivering 300 million doses of safe and effective COVID-19 vaccines in less than approximately 20 percent of the normal vaccines development, production and distribution time.

Smith worked within OWS' Security and Assurance (S&A) element.

She developed a comprehensive training program attended by approximately 100 DCSA industrial security representatives, Army Counterintelligence personnel, and OWS security personnel, forming the cornerstone for OWS security support in the field. This singular training event set the direction and completion of more than 17 on-site evaluations conducted in the midst of the pandemic at facilities with little understanding of the threat and with minimal security programs in place. She also co-authored the risk assessment questioning protocol to drive OWS's evaluation of security and counterintelligence vulnerabilities across seven security disciplines. This protocol established a consistent approach by multiple agencies at every industry engagement and standardized critical site-specific assessment data points back to OWS S&A, informing the unique task force's risk methodology.

**W**hile serving as curriculum manager for Counterintelligence at CDSE, Kobeski proved an invaluable asset to the National Counterintelligence and Security Workforce throughout 2020. His support to National Supply Chain Integrity Month (NSCIM) provided a vital, virtual outlet for critical information during a global pandemic, and delivered quality information and training on multiple Counterintelligence topics, keeping the workforce prepared.

He was a key communicator for supply chain associated information intended for the security community during the onset and continuation of the COVID-19 pandemic; specifically as supply chain concerns became a major issue on both the national and world news. He aggressively supported the National Counterintelligence and Security Center's NSCIM in April 2020 by developing two

webinars with expert guests, preparing new CI course curriculum content, and then working with CDSE Communications team to put out social media messaging to support supply chain awareness.

Between the two supply chain webinars, the attendees downloaded 430 supply chain-related job aids and files, and on-demand viewers watched these webinars 142 times throughout 2020. Kobeski was directly responsible for the creation of a new Supply Chain Threat poster to increase awareness and assist the local security managers with supply chain reporting; a Supply Chain-centric CDSE Pulse newsletter; and over 10 updates to the Supply Chain toolkits on the CDSE.edu website.

Kobeski proficiently managed numerous products and projects regarding CI threat awareness, including a catalogue of nine e-Learning courses, four shorts, nine job aids, and 10 case studies. This also included developing a new e-Learning course, maintenance on four older e-Learnings and two security shorts, preparing to teach classes for DCSA CI's Introduction to CI course, and development and delivery of five webinars (to include two for NSCIM). The webinars resulted in 786 downloaded files, 2,501 live views, and representation from 14 countries outside the continental United States.

---

**T**he CDSE Insider Threat Division provided expert training and awareness to the CI community in 2020 by hosting products generating over 1,000,000 views, while releasing 44 new products to include the Insider Threat Sentry Application, developing graduate level instruction, supporting Operation Warp Speed, and hosting the Insider Threat Virtual Conference.

In 2020, the Insider Threat Division took an innovative approach to achieving its mission of increasing the availability of its awareness materials by launching the Insider Threat Sentry Application. Designed for use on commercial portable electronic devices (PED), it streamlines access to CDSE's

library of Insider Threat awareness materials for security professionals. Users can quickly find and download resources such as posters, videos, security awareness games, vigilance campaign kits, exclusive content, and more to enhance Insider Threat programs and spread awareness.

In July 2020, CDSE coordinated with Office of the Under Secretary of Defense for Intelligence and Security (OUSD (I&S)), Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and Health and Human Services to develop a job aid, "Insider Threat Implementation Guide for Healthcare and Public Health Sector," for Operation Warp Speed (OWS) partners. The job aid supported the development of Insider Threat risk programs within those critical sectors.

CDSE partnered with the NCSC, National Insider Threat Task Force, OUSD (I&S), DHS, DCSA, and community stakeholders to support National Insider Threat Awareness Month (NITAM) 2020 activities. In the summer of 2020, CDSE launched the NITAM website. Designed to optimize both stakeholder and participant involvement, the NITAM website included games, videos, social media graphics, posters, case studies, scenarios, news, articles, and endorsements from OUSD (I&S), the NCSC Director, and the DCSA Director. Since its launch, the website has received acclaim from stakeholders and participants alike with close to 6,000 visits within the first few days of going live.

The 2020 Virtual Insider Threat Conference served as another successful initiative during NITAM. With 1,700 participants from across the globe, CDSE hosted an all-day conference with a full agenda of topics including an Insider Threat program update, industry policy, a detailed case study briefing, and research support and best practices for building resilience.

# NEW RATING MODEL DESIGNED TO COUNTER THE THEFT OF CRITICAL PROGRAM AND TECHNOLOGIES

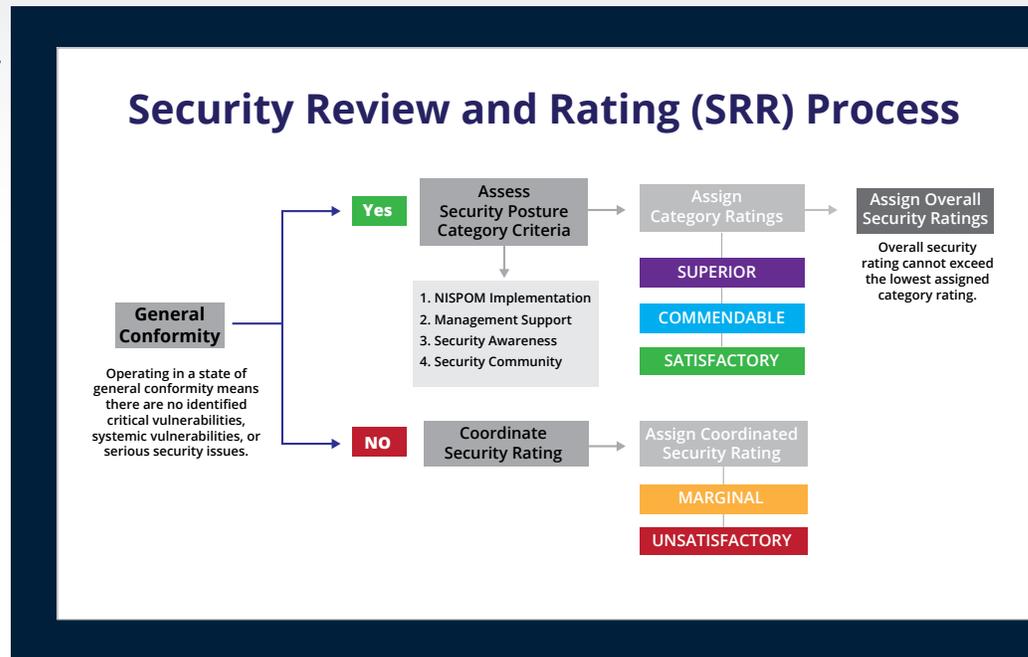
**L**ong before the COVID pandemic, the Critical Technology Protection directorate (CTP) was wrestling with how to make it harder for our adversaries who were stealing critical program information and technologies. Without a clear whole-of-government strategy available, the CTP security experts chose to create one, DCSA in Transition (DiT). After three years of DiT research and development, the CTP

team thought they had an answer, but in March 2020, while leading efforts to develop a single review model known as the Security Review and Rating (SRR) Process, the pandemic shut down operations.

CTP pivoted and asked the fundamental question — how would they ensure that 12,500 cleared contractors were compliant with 32 CFR Part 117 NISPOM Rule during a pandemic. CTP security experts agreed that the Continuous Monitoring Engagement (CME) model was the answer. It enabled DCSA's ability to conduct remote verification of industry compliance with the NISPOM Rule and requirements to safeguard classified information at their facilities. The CME built on National Access Elsewhere Security Oversight Center (NAESOC) virtual continuous monitoring engagement procedures already in place for the companies that access classified information at government or other industry locations. NAESOC is designed to provide consistent oversight and security management for select facilities that do not possess classified information on-site, requiring access elsewhere.

"It's been very effective and the CME's success surprised a lot of people in its ability to produce results. DiT produced the NAESOC and NAESOC produced the CME process that enabled us to continue to provide oversight of industry from afar in a virtual environment the best we could during a pandemic," said Matthew Roche, CTP Operations Division Chief. Over the course of 18 months, DCSA conducted more than 10,000 CMEs at nearly 8,000 different corporate or business facilities.

While using CMEs to provide remote oversight of companies during the pandemic, the CTP team reevaluated the DiT model. CTP was intent on taking the opportunity that COVID provided to complete the design of a single review model to protect critical technologies and programs. The refined security review approach





incorporates best practices from previous security review models and functions within the DCSA charter and NISPOM Rule compliance while identifying risks posed throughout classified contract performance. Security reviews are conducted based on national level priorities (DoD Critical Program and Technology List) and risk management. CTP personnel review internal processes with contractor personnel throughout classified contract deliverable lifecycles to assess NISPOM Rule compliance, determine if measures are in place to counter potential threats, identify vulnerabilities and administrative findings, and advise the contractor on how to achieve and maintain an effective security program.

CTP provides a formal security rating at the conclusion of the security review that reflects the contractor's effectiveness in protecting classified information. The refined security rating model is a criteria-based system that aligns processes, terms, definitions and minimum rating requirements to DOD and national level policy. Lastly, the security rating process is a compliance first model that eliminates the use of enhancements and uses a whole company approach based on a corporate culture of security to include management support, employee awareness and cooperation within the security community. Roche coined the phrase "whole company approach" from a similar concept and terminology related to personnel security adjudications based on the "whole person."

On Sept. 1, 2021, DCSA's Security Review and Rating Process took effect. CTP's security experts briefed industry representatives — answering their questions on the ratings process, including new criteria to be applied during security reviews — via live webinars. However, CTP continued to monitor companies virtually, to include conducting interviews with facility security leads to determine their security postures. Although effective, CME engagements can't replace an on-site security review since there are security review components that must be completed at a facility by DCSA industrial security representatives. As a result, CTP envisions that CMEs will be complementary to the security review in the future.

One of the CTP security experts deeply involved in development of the new rating process is Misty Crabtree of the Virginia Beach Field Office. "We took the best practices from DiT and incorporated those into this methodology while making sure that we stay within the bounds of policy," said Crabtree, senior industrial security representative. "It's a breath of fresh air for industry and agency personnel because it really does bring us back to what we do best which is oversight and making sure that classified information and classified contract deliverables are being protected throughout their lifecycle."

"Compliance with NISPOM comes first," said Crabtree, one of 190 industrial security field representatives throughout DCSA's four regions. "If a company is compliant and determined to be in general conformity, that's

when we look at the whole company approach, which means that we are no longer just looking at the facility security officer or the security staff and providing a rating based on their implementation of the program.”

At that time, Crabtree and her industrial security colleagues apply the whole company assessment based on the company's culture of security, including management support, employee awareness and cooperation within the security community. The final step is a formal security rating that reflects the contractor's effectiveness in protecting classified information; superior, commendable, satisfactory, marginal or unsatisfactory.

“It truly is a whole company effort to receive a higher level security rating,” said Crabtree. “The management within the organization must be aware and make decisions based on threat. They must understand what the threat is and fully support the security program while embedding a culture of security. It requires the employees and management – all the way through the organization – to do their part.”

DCSA security professionals combine their experience, training and professional standards with information collected and knowledge obtained during the normal progression of the security review to carefully analyze the category criteria.

“This includes making a rating determination using ethical principles of objectivity; not allowing bias, conflict of interest, or the influence of other people to affect their decisions or actions,” said Crabtree. In other words, the SRR process ensures all companies have the same opportunity to achieve superior ratings. Security review and ratings provide information sharing and feedback opportunities to help industrial security partners improve their internal processes and overall security program.

“Our partnership with industry is critical,” said Roche. “This single security review model is an effort to provide industry with consistency and predictable engagements that they welcome. It's a valuable management tool and that's really what we're after - to stand shoulder to shoulder with industry and get the absolute best results we can.”

As DCSA strives for consistency in processes, the agency's industrial security representatives understand that outcomes may vary based on facility circumstances. “Our security professionals will document their rationale for the conclusion within their security review report,” said Crabtree. “Then, using our recently updated quality management program, we will continuously monitor consistency throughout the agency, readjust and train as needed. Ensuring clear professional standards are outlined and achieved is extremely important to DCSA.”

# Asking the right question yields better interview results

Editor's Note: The following reflects the thoughts and opinions of the author on the importance of productive interviewing as part of security reviews.

By *Dave Bauer*  
*Critical Technology Protection*

---

In a Pink Panther movie, detective Inspector Jacques Clouseau approaches a man with a dog sitting next to him. In his characteristic French accent, Inspector Clouseau asks the man, "does your dog bite?" The man answers "no" and the Inspector bends down to pet the dog, only to be bitten. Inspector Clouseau snaps, "I thought you said your dog did not bite!" The man answers, "That is not my dog."

When I assumed my current role as CTP Western Region Director, I understood I was stepping into a different arena. I had spent much of my career in the counterintelligence and counter terrorism fields. As with any new job, I hoped to contribute to the great work that was already underway and an area I believed I could influence was productive interviewing. When I arrived, I would advocate whenever possible we (DCSA Industrial Security) needed to train the curiosity back into our workforce. We immediately launched new training for industrial security representatives and information systems security professionals on developing interviewing skills. The specific purpose was to learn best practices and strategies from career investigators on how to ask probing questions, read body language, listen to the tempo in the response, identify future leads that needed to be followed up on, and make judgements on further lines of questioning.

This interview skill is even more important as DCSA embarks on the Security Review and Rating model and as we re-establish on-site reviews. The main objective of DCSA's security review process is simply centered on facility leadership and programs protecting national security information as outlined in 32 CFR Part 117 NISPOM Rule and are they able to identify and defend against illegal collection efforts by potential adversaries. Our collective objective is

to deliver an uncompromised product or capability to the warfighter or other U.S. government agency.

Interviews are the most essential factor in providing our leadership, government customers, and the facility a valid evaluation. That's why we need to talk to more people about the right things within industry during our security reviews, with a specific purpose in mind and value the time of the interviewee. I am convinced our unified success is tied to how well we ask questions, listen to the response; then ask the appropriate follow up question, and again listen to the response until we are satisfied the purpose behind the question has been answered.

For instance, when DCSA representatives ask a facility security officer whether they have an effective insider threat program, DCSA and the cleared contractor need to understand the purpose behind the answer. I suggest the ultimate purpose behind an insider threat question be designed to determine their effectiveness of defending against an internal nefarious act. So asking whether the facility has an insider threat program and a senior management official is important, but it's not enough and does not achieve the purpose of the security review. These questions will take us closer to having confidence in the effectiveness of a program.

In preparing for an engagement, but especially critical during the new Security Review and Rating process, thoughtfully prepare your interview subject listing to focus on personnel you believe are at most at risk because of the nature and sensitivity of their jobs or have oversight of critical security program parts. Then ask the probing questions that provide you the insight necessary to make a judgement.

**“I thought you said  
your dog did not bite!”**

**The man answers,  
“That is not my dog.”**

~ The Pink Panther Movie

Here are some probing questions to consider:

Interviewee	Probing Questions
<p>Business Development</p>	<ul style="list-style-type: none"> <li>• Describe your role in developing future business opportunities? Where do you travel?</li> <li>• How do you protect yourself against only disclosing approved information when you are asked questions?</li> <li>• Describe the difference between what you are authorized to discuss concerning this project?</li> <li>• Have you ever had to say, no to an inquiry, I cannot divulge that information? If yes, describe the circumstance.</li> <li>• Are you comfortable saying no in your job? What would make it easier?</li> </ul>
<p>Foreign Visit Hosts</p>	<ul style="list-style-type: none"> <li>• What has been the background and purpose of your visitors?</li> <li>• How much do you know before the visit occurs?</li> <li>• What were the interesting questions or discussions outside the purpose of the visit?</li> <li>• How do you prepare for hosting?</li> <li>• Did you give a walking tour? If yes, where did you walk?</li> <li>• Have you heard back from any of the visitors?</li> </ul>
<p>Subject Matter Experts (Technology)</p>	<ul style="list-style-type: none"> <li>• How do you receive invitations to speak at domestic or international conferences? What is your attitude towards attending conferences, are they important to you? Why?</li> <li>• Do you have a group of common associates in your field? How did you meet? How do new experts get into your group?</li> <li>• How do you recruit people as part of your team? How often do you lose people off your team? Why?</li> </ul>

In the end, when a DCSA industrial security representative finalizes a security review, DCSA is validating the facility has an effective security program and moreover, has developed a culture that is agile and is committed to protecting national security. And as Inspector Clouseau found out, an important part of that process is an appropriately framed question to the right people about the right things.

Interviewee	Probing Questions
<div data-bbox="155 569 764 957" style="border: 1px solid black; border-radius: 15px; padding: 10px; text-align: center; margin-bottom: 10px;">Human Resource</div>	<ul style="list-style-type: none"> <li>• Describe how you hire new employees? Do you go to specific pools of candidates, such as local universities or other sources?</li> <li>• How do you select a candidate for a position of trust within your facility? What checks are done? Describe a potential hire that was denied?</li> <li>• How often do you get feedback from a supervisor on a new employee and behaviors that may be an indication of trustworthiness issues (i.e. tardiness, distracting behavior, etc.)</li> </ul>
<div data-bbox="139 957 708 1293" style="border: 1px solid black; border-radius: 15px; padding: 10px; text-align: center; margin-bottom: 10px;">Cleared Employee</div>	<ul style="list-style-type: none"> <li>• If I entrusted you with a classified document you needed for your job, what would you do? Walk me through the process.</li> <li>• Do you work on both classified and unclassified programs that have common aspects? If yes, how do you protect against inadvertent disclosure when working on both? Are you confident in knowing the difference?</li> <li>• What was the name of your security education presenter? Was the presenter effective? Tell me one or two things you remember from the training?</li> </ul>
<div data-bbox="147 1293 732 1661" style="border: 1px solid black; border-radius: 15px; padding: 10px; text-align: center;">Insider Threat</div>	<ul style="list-style-type: none"> <li>• How often has your insider threat working group met?</li> <li>• What were the triggers to empanel the insider threat working group?</li> <li>• How many potential insider threats were identified?</li> <li>• How many of those were deemed nefarious?</li> <li>• Describe how you determined the nefarious from the non-nefarious?</li> <li>• How did you notify the Government Contracting Activity of the nefarious actor?</li> </ul>

# BUILDING RELATIONSHIPS WITH KEY MANAGEMENT PERSONNEL (KMP)

*By Senior Industrial Security Representative Tameka Watts  
Critical Technology Protection*

**R**elationships in life are important as they create a level of stability and trust which enables a person to function effectively. The same is true for business relationships. Facility security officers (FSOs) face challenging roles while managing security programs; however, building and maintaining strong relationships with key management personnel (KMP) can ease daily stress.

The KMP are defined, per the 32 CFR Part 117 NISPOM Rule, as “an entity’s Senior Management Official (SMO), Facility Security Officer (FSO), Insider Threat Program Senior Official (ITPSO), and all other entity officials who either hold majority interest or stock in, or have direct or indirect authority to influence or decide issues affecting the management or operations of, the entity or classified contract performance.” The number of KMP at facilities can range from one to greater than 10 and an individual relationship with each KMP is essential in continuously improving security program knowledge and sustaining a strong and effective security program.

The FSO is in a unique position in which they must supervise and direct measures of the NISPOM Rule and U.S Government requirements to protect classified information. The FSO must have firsthand knowledge and a solid understanding of their facility’s business which can only be achieved through relationships. Attempting to build relationships with higher level positions can be daunting and a challenge that seems impossible; however, the following three simple steps can develop and maximize relationships: Introduction, Communication and on-going Maintenance.

## **Step 1 - Introduction:**

Taking the opportunity to proactively engage KMPs at the facility and conducting mutual introductions is a great start in establishing long lasting partnerships. Face-to-face introductions may not be possible for a variety of reasons, but email and telephonic introductions are a great start and are very effective. Creating a written plan on different topics to discuss including individual roles is an excellent preparation tool. Actively engaging and asking questions about the overall business is another great way to kick-off the discussion.

## **Step 2 - Communication:**

Communication is the absolute key for continued development and growth. Engaging KMPs and continually collaborating on areas of focus for their security program for the specific year and further explaining those key areas of the security program that DCSA is tracking and measuring could really make a significant difference in their security program. This step not only empowers the FSO, but also builds trust within the various levels of management and opens the door for collaboration.

Knowing your audience will determine how you communicate whether via an open discussion or via a presentation; regardless, it is necessary to do so in the manner that best fits the topic.

## **Step 3 - Maintenance:**

A few meaningful conversations with KMPs to emphasize the benefits of a strong security program to include discussing progress on security program initiatives, challenges, self-inspections, results of staff interviews, vulnerabilities/findings discovered/ongoing mitigation, engagements with DCSA/cognizant security agencies or outcomes from security education efforts could really impact the security staff and their security program.

It is never too late to establish or maintain an effective relationship with KMPs. The benefits outweigh the fear and will only enhance your security program. The FSO as a KMP has a level of influence over the business whether small or large and the FSO’s voice is important for all business decision making. Make it a goal to use every interaction to enhance relationships even if you are always the person initiating the conversation because in the long run, it will be worth it.

# REPORT INTERNATIONAL SECURITY VIOLATION IF LOSS, COMPROMISE OF FOREIGN GOVERNMENT INFORMATION

By Matthew Sergent  
Critical Technology Protection

The Defense Counterintelligence and Security Agency serves as the Cognizant Security Office providing oversight to approximately 12,000 cleared U.S. companies under the National Industrial Security Program (NISP), on behalf of the Secretary of Defense. In this capacity, DCSA ensures the security of U.S. government and foreign government sensitive and classified information, technologies, and material entrusted to cleared industry.

As a part of these security oversight duties, industrial security representatives (ISR) work with cleared contractors to protect foreign government information (FGI) as they would U.S. classified information. Discovery of compromises to and/or loss of FGI constitutes an international security violation that requires cooperation and reporting by the cleared industry partner and DCSA ISRs. What follows is an overview of the international security violations reporting process.

Is it an International Security Violation?

A security incident becomes an International Security Violation when it involves the loss, compromise or suspected compromise of FGI. FGI is defined in the 32 CFR Part 117 NISPOM Rule as information "...provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or produced by the United States pursuant to, or as a result of, a joint arrangement with a foreign government or governments, an international organization of

governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence."

The first step is for the contractor to notify the ISR of the security incident and open a preliminary inquiry to determine the exact nature and scope of the incident. During the preliminary inquiry, the contractor determines if FGI is involved. If the security violation involves FGI, the contractor should review the requirements found in 32 CFR 117.8(d) because International Security Violations follow similar reporting requirements as standard US security violations.

32 CFR 117.8(d) requires the contractor to write an initial report which should include the following: 1) the cause of the incident; 2) determination of the information classification; 3) determination of whether the information is FGI; 4) determination of information systems affected; 5) immediate steps taken to secure the information at risk; and, 6) next steps to be taken as the inquiry progresses to the final report.

Once completed, the contractor will submit the Initial report to the Cognizant Security Authority (CSA) as per 32 CFR 117.8(d). When submitted to DCSA, the ISR will verify the information in the initial report. Key facts to verify in the initial report are:

- Data owner/foreign country (country's classified information that was involved)
- Program information (example, F-35 Joint Strike Fighter)
- Government point of contact information
- Specify where spill originated, i.e., foreign country or U.S.

The ISR will then log the initial report into the National Industrial Security System (NISS), and forward it to DCSA's International and Special Programs Division (ISP) for action.

The contractor will continue the investigation until all applicable facts are discovered. Facts not available during the preliminary inquiry and/or discovered during the investigation are incorporated into the contractor's final report. The final report is due to the CSA when the investigation is completed as per 32 CFR 117.8(d). Requirements for the final report are outlined in 32 CFR 117.8(d)(3), include:

- Material and relevant information not included in the initial report.
- The full name and social security number of the individual or individuals primarily responsible for the incident, including a record of prior loss, compromise, or suspected compromise for which the individual had been determined responsible.
- A statement of the corrective actions taken to prevent a recurrence.
- Disciplinary action taken against the responsible individual or individuals, if any.
- Specific reasons for reaching the conclusion that loss, compromise, or suspected compromise did or did not occur.

If submitted to DCSA, the DCSA ISR will review the report, log the final report into NISS, and forward it to ISP Division (ISP) within five working days for interagency coordination.

ISP will coordinate the report with the Defense Technology Security Administration (DTSA). 32CFR Part 117 NISPOM Rules outlines DTSA's responsibility

to notify the appropriate foreign government of the loss or compromise. Industry partners are required to follow any recommended mitigation strategies and coordinate efforts required to secure the information.

Contractors and ISRs should treat International Security Violations with the same rigor as standard security violations involving U.S. classified information, and follow the processes and procedures for reporting suspected loss or compromise of FGI.

# ANNUAL FOCI CONFERENCE SPEAKERS FOCUS ON FUTURE, ADAPTING TO GREAT POWER COMPETITION

*By Ana Francisca Regalado and Tracy Rixmann  
Critical Technology Protection*

DCSA's mission to mitigate foreign ownership, control or influence (FOCI) is changing to meet the evolving risk landscape, as discussed during the 25th Annual FOCI Conference on August 18, 2021. Despite COVID-19 challenges, DCSA committed to continuing the event virtually for the second year in a row, hosting over 800 FOCI industry and government stakeholders. This year's conference focused on strategic changes coming to the FOCI program.

During the FOCI Process panel, Matthew Kitman, operations officer for Entity Vetting (EV), explained the shift coming to the FOCI process is due to not only updates with the release of 32 CFR Part 117, NISPOM Rule, but because the U.S. government has been focused on the need for increased industrial security and economic security.

"No longer are we on a battlefield necessarily just in Afghanistan or Iraq," Kitman said. "We are in non-kinetic battles with some of our adversaries, and the requirements and the work that you do is meant to assist our warfighters in winning all of those battles." The FOCI program continues to evolve with mitigation strategies that can best benefit the U.S. government and cleared industry, and ultimately protect their information from adversaries and competitors.

Dustin Dwyer, Mitigation Strategy Unit chief (MSU), discussed concerns over foreign suppliers being appropriately mitigated. "Non-traditional business relationships and subsidiary operations that are

normal for a multinational corporation operating overseas may be a benefit to the company, but could pose a potential risk for foreign influence," he said.

The DCSA scope of mitigation is widening to include greater aspects of foreign influence, such as foreign suppliers who without FOCI mitigation, could have the ability to adversely affect contractor performance. With a focus on foreign suppliers, industry will see DCSA start to build additional tools and requirements into mitigation strategies. For example, Dwyer discussed a requirement ensuring government end users or customers are informed when a company is using foreign suppliers or manufacturing outside the United States.

The panel emphasized, as always, DCSA welcomes any conversations to determine the best mitigations for each company that suits the U.S. government and contractor's legitimate interests.

During the Cybersecurity Maturity Model Certification (CMMC) and Controlled Unclassified Information (CUI) session, John Massey, deputy assistant director for Enterprise Security Operations, provided an overview of the CUI program. While CUI may not necessarily be classified, the information still requires protection from unauthorized disclosure, including disclosure to a foreign parent company. Massey emphasized that industry can lean forward by reporting instances of unauthorized disclosure to DCSA.

**“ We are in non-kinetic battles with some of our adversaries, and the requirements and the work that you do is meant to assist our warfighters in winning all of those battles.”**

~ Matthew Kitzman

Keynote speaker DCSA Director William Lietzau highlighted the unique and important role FOCI companies play in strengthening security programs within the National Industrial Security Program, including the vital role and services they provide to U.S. government agencies. “The work that we are doing in FOCI has never been more important,” he said.

As DCSA adapts to new threats affecting U.S. critical technology infrastructure and its economic security, great power competition has garnished DCSA’s attention. To which Lietzau called on the oversight and strategic direction from Outside Directors, security professionals, and corporate executives to combat pressures and effects of foreign competition in the U.S. defense industrial base.

The director concluded by emphasizing the significance of forging stronger partnerships between industry and DCSA for the success of the DCSA missions.

Dustin Gard-Weiss, Deputy Director of National Intelligence (DNI), detailed the importance of relying on the private sector in the deployment of preventative technological measures that ensure the protection of our national security. “The supply chain that is feeding the national industrial security program – that’s where the threat has a much easier way of getting in today than any time before,”

he said. To address this, Gard-Weiss asked for the private sector to engage more and become the first responders in the front lines to safeguard the infrastructure of this country.

The success of national and economic security programs rely on the diversity of industry sectors. Gard-Weiss advocated the removal or reduction of challenges for the private sector without jeopardizing our national security. One method he discussed was the imperative to increase information sharing capabilities with industry partners. Gard-Weiss concluded by stating that we need industry to keep evolving its technology so that the United States can maintain an asymmetric advantage over its adversaries.

Christopher Forrest, acting assistant director for EV, concluded the conference by echoing Lietzau’s message of promoting and forging partnerships between industry and DCSA. Forrest expressed his gratitude for the collaboration between DCSA, Outside Directors, Proxy Holders and everyone whose job is to promote the security measures in the cleared defense industrial base. He affirmed that despite the challenges imposed on the agency by the pandemic, “we will all continue to work collectively and utilize one another as a force multiplier to achieve the success and mission of DCSA.”

# CONDITIONAL ELIGIBILITY DETERMINATIONS SAVE TIME, RESOURCES BY LEVERAGING USE OF CONTINUOUS VETTING TECHNOLOGIES

*By Benjamin J. Schultz*  
*DCSA Adjudications*

In November 2021, DCSA Adjudications reintroduced the Conditional Eligibility Determinations adjudicative process to save on time and resources by diverting qualifying military and civilian cleared individual cases into a process that leverages newly interlinked DCSA directorates and technologies.

This process is based on a successful pilot with the Department of the Navy's military members and civilian personnel that confirmed the viability and proposed benefits of the process. Conditional Eligibility Determinations use the Continuous Vetting (CV) technologies executed by DCSA Vetting Risk Operations (VRO) to reduce the initiation of certain due process proceedings in favor of security monitoring.

A cleared individual may be granted a Conditional Eligibility when an adjudicator determines that the information is serious enough to warrant a recommendation of denial or revocation of national security eligibility, but the specific risk to national security can be managed with appropriate mitigation measures. Only issues related to the following five Adjudicative Guidelines (as defined by the Security Executive Agent Director (SEAD) 4) — Sexual Behavior, Financial Considerations, Alcohol Consumption, Drug Involvement and Substance Misuse, and Criminal Conduct — may warrant a Conditional Eligibility Determination.

For qualifying cases, the cleared individual of investigation agrees to conditions set forth in correspondence from DCSA Adjudications sent to them and their command and to being monitored by CV. This will not impact normal execution of due process, but will divert cases that could be considered on the "borderline" between granting and removing eligibility. For a period of one year, VRO monitors the individual's Conditional Eligibility for repeat offenses or subsequent derogatory behaviors as cited in the correspondence, to which they agreed. If such derogatory behavior is identified, the record is provided to DCSA Adjudications for expedited adjudication and/or issue resolution as appropriate. If there is no derogatory information identified in the subsequent year, DCSA Adjudications removes the "Condition" from the case management and adjudications system and enters a final favorable eligibility.

The implementation of Conditional Eligibility determinations with the current and evolving monitoring capabilities at VRO not only improves overall mission readiness for our customers, but also provides enhanced oversight and risk management to the national security community.



# ADJUDICATIONS INCIDENT REPORT GUIDE FOR SECURITY MANAGERS

*By Charles Peterson, Team Chief and Mary Lee, Branch Chief  
DCSA Adjudications*



In an effort to ensure the security of classified information or technology, security managers and facility security officers (FSOs) are required to report any adverse information that comes to their attention concerning a cleared employee. Adverse information consists of any information that negatively reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security. In reporting the incidents, it is imperative that security managers and FSOs provide all information that is available so that DCSA Adjudications is able to make a well-informed decision.

## **Details are important**

Security managers and FSOs can create, submit, and update incident reports in the Defense Information System for Security (DISS) on cleared personnel reporting events that may affect the individual's eligibility to access classified information. When creating a new incident, in the Incident Notes, be as thorough as possible, but at a minimum, provide the five W's (Who, What, When, Where, and Why). The five W's help to explain the 'Who was involved,'

'What happened,' 'When it happened,' 'Where it happened,' and 'Why it happened.' For example, instead of "John Doe was driving under the influence (DUI)," the following is preferred: "Mr. John Doe had a DUI on Friday, October 15, 2021, while driving home from a party; he was arrested by the Localville Police Department and released with a court date not yet determined. Local access was not suspended."

## **Supporting documentation**

When providing reportable information, submit all available supporting documentation. For instance, if the individual has financial problems, it would be appropriate to submit correspondence with creditors, copies of bankruptcy filings, and copies of canceled checks. If the subject had a security violation, provide letters to the subject from security, commander/director, etc., as well as any related training completed (both before and after the incident). If the subject tested positive for an illegal drug, provide test results, letters to the subject from security, commander/director, etc., and results of any investigation conducted. Security managers and FSOs play an important role in providing information and supporting documentation assisting adjudicators in making timely adjudicative decisions.

### **Valid, responsive points of contact**

Communication is vital to the personnel security vetting process. Security managers and FSOs are the keystone to its success and play a critical role in communicating with DCSA, as they interact with cleared individuals on a frequent basis. All of these steps are important.

Finally, when submitting the IRs or CSRs, it can't be overstated how important it is that a valid and responsive points of contact (POCs) be provided for Adjudications to communicate with on submissions. While it's good that there are general POCs identified in DISS, identifying yourself and how we may contact you about your request/submission (such as phone number and email address) can often help expedite processing of the request/submission. With valid and responsive POC information, DCSA Adjudications can call or email for additional information if needed. General organization, office email address, or a phone number that leads to a general options tree ("for English, press one..."), greatly slows down the processing of requests.

In closing, providing relevant and appropriate details with supporting information and specific points of contact is very important and enhances the ability to provide a timely decision.

# CUSTOMER ENGAGEMENTS TEAM PROVIDES CUSTOMER SERVICE SUPPORT FOR IT SYSTEMS

*By Amanda Grossman  
Background Investigations*

**H**aving an issue with the Defense Information System for Security (DISS)? You're not alone but DCSA is taking action to help. In July 2021, the Customer Engagements Team (CET) was created to provide customer service support for three key IT systems used by DCSA customers: DISS, Defense Central Index of Investigations (DCII), and Secure Web Fingerprint Transmission (SWFT).

These systems were previously supported by the Defense Manpower Data Center which relied on contractor support to staff the call center. However, when the systems transferred to DCSA, the decision was made to federalize this support desk as the support contract expired. In an effort to rapidly staff the center with a federal workforce, the Background Investigation's Customer & Stakeholder Engagements division organized resources from across the DCSA landscape. Eventually, 26 personnel received training on these three systems and prepared the CET to support customers beginning in early August 2021.

In the short time that the CET has been answering queries on DISS, DCII and SWFT, the team has worked diligently to reduce the average wait time for callers. In the first three months of support, the CET has taken 33,324 phone calls with an average customer wait time of only 15 seconds. The dependability of this team enhances the agency's customer relationships as they have come to rely on the CET to answer their calls in a professional and timely manner and also provide expert support for their questions and concerns.

## What are they?

- DISS serves as the enterprise-wide solution for personnel security, suitability, and credentialing management for DOD military, civilian, and contractors. It is a web-based application that provides secure communications between adjudicators, security officers, and components, allowing users to request, record, document, and identify personnel security actions.
- DCII is an automated central index that contains investigations conducted by DOD investigative agencies, and personnel security determinations made by DOD adjudicative authorities. DCII access is limited to DOD and other federal agencies that have adjudicative, investigative, and/or counterintelligence missions.
- SWFT enables cleared Defense industry users to submit electronic fingerprints (e-fingerprints) and demographic information through SWFT to DCSA's Fingerprint Transaction System (FTS) for individuals who require an investigation by DCSA for a personnel security clearance.



During this time, the CET has also been able to build partnerships with many teams across the agency. By building working relationships with DCSA's National Background Investigation Services team, Program Executive Office, Vetting Risk Operations (VRO), and the DCSA Adjudications, the team has been able to identify process improvements, such as the ServiceNow ticketing system, to adapt to the needs of the customers. If the team is unable to provide resolution for the customer while assisting them on the phone or through email, issues are escalated to the appropriate next level support group for follow-up and resolution.

Additionally, the CET absorbed the existing Applicant Knowledge Center and is now supporting applicants in e-QIP on behalf of VRO. Due to the impacts of COVID restrictions, the VRO team did not have the capability to answer calls while teleworking. As a workaround, the CET answered over 140,000 industry customer calls in fiscal year 2020 and over 152,659 calls to support e-QIP users as they navigated the application in fiscal year 2021.





**With less than a year in operation, the CET continues to provide first line support and is ready to support customers across the federal space.**

Contact the Applicant Knowledge Center  
via phone: 724-738-5090  
via email: [DCSAAKC@mail.mil](mailto:DCSAAKC@mail.mil)



# Defense Counterintelligence and Security Agency

27130 Telegraph Road  
Quantico, Virginia, 22134  
DCSA.pa@mail.mil  
571-305-6562  
[www.DCSA.mil](http://www.DCSA.mil)