Official Magazine of the
Defense Counterintelligence and Security Agency

# Gatekeeper

Volume 1, Issue 3

# DCSA SUPPORTS SOUTHERN BORDER MISSION

## IN THIS ISSUE

# IN THIS ISSUE






## VOL 1 | ISSUE 3

## DCSA Gatekeeper

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

27130 Telegraph Road
Quantico, Virginia, 22134

DCSA.pa@mail.mil
571-305-6562





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 publica tion is the responsibility of OCCA.

All pictures are DOD photos, unless otherwise identified.

# FROM THE DIRECTOR

The cover story of this issue again demonstrates the widespread relevance of DCSA's work. Not only is our enduring security work of unparalleled importance to our nation's future security, we are also directly involved in the ever-changing events of the day. In the last issue of Gatekeeper, we described DCSA's work on Operation Warp Speed — the program supporting the development of vaccines that have allowed our country to bounce back faster than any other from the pandemic.

In this issue, we review the support our Background Investigations Directorate is providing to the Department of Health and Human Services (HHS) and U.S. Public Health Service (USPHS) Unaccompanied Minor Resettlement Program. Child care security reviews are one of the many products we offer our government. Required by law, they are also critical to the safety and security of these children at our border. I am proud that DCSA was able to quickly adjust and support this program. It provides another example of the dedication and commitment of the DCSA workforce.

These pages also reflect the breadth and complexity of the DCSA mission set: International Programs; Unauthorized Disclosure; Insider Threat; oversight of the IT systems in industry; and oversight of Controlled Unclassified Information—a new mission. These disparate programs all fall under the security umbrella that defines DCSA.

I also want to highlight the short article on the migration from the Joint Personnel Adjudication System (JPAS) to the Defense Information System for Security (DISS). This transfer was not without its challenges. Indeed, we recognized a number of technical issues soon after DCSA adopted the DISS program, and we delayed migration for several months to allow the team to work through as many of those issues as possible. Although users are still learning their way around DISS, and they may have preferred to use JPAS for longer, continued reliance on that system was simply not feasible. JPAS was established in February 2001, having evolved from the U.S. Air Force Sentinel Key program that started in October 1998. Our DISS team still has work to do, but they are committed to continuing to enhance DISS while listening and responding to user concerns.

As we move through the summer, we see COVID-19 restrictions being lifted across the country. Our investigators, industrial security representatives, information system security professionals and counterintelligence special agents will begin to return to in-person interviews and industry engagements. Although returning to field work is exciting and necessary for accomplishing our mission effectively, it will require adjustments and new ways of interacting with one another. Safety and good judgement should mark our deliberate and responsible movement through the next phase.

Thank you for reading, and thank you for your continued support to DCSA.

William K. Lietzau
Director,
Defense Counterintelligence
and Security Agency

# ASK THE LEADERSHIP

## Dr. Ronzelle L. Green

Chief Information Officer

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

Dr. Ronzelle L. Green is the chief information officer for DCSA, where he is responsible for the development, implementation, and operations of information technology (IT) designed to enable the agency's mission.

Prior to joining DCSA, Dr. Green served as the director of Commonwealth integration at Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), where he was responsible for integrating Commonwealth partners into the Defense Intelligence Enterprise. Prior to that assignment, he served as the director of the international solutions office at the National Geospatial-Intelligence Agency (NGA), where he led the acquisition, development, and operations of IT to enable a collaborative geospatial intelligence relationship with international partners. He has held senior IT, engineering, and operational roles within government, industry, and the military. Dr. Green is also a professorial lecturer in the School of Engineering and Applied Science at The George Washington University.

Dr. Green is a United States Coast Guard reserve captain, currently assigned as the Coast Guard senior advisor of the Navy Expeditionary Combat Command (NECC) at the Joint Expeditionary Base Little Creek. Previous assignments include the Joint Chiefs of Staff at the Pentagon; commander, Maritime Security Detachment, Guantanamo Bay, Cuba; commanding officer, Port Security Unit 308; executive officer, Port Security Unit 305; senior intelligence officer, Coast Guard Cryptologic Group, National Security Agency (NSA); assistant chief of intelligence, Coast Guard Deployable Operations Group, and other assignments.

Dr. Green received a B.S. from Oral Roberts University, an M.S. from North Carolina State University, an M.S. in Strategic Intelligence from the National Defense Intelligence College, and a Ph.D. in Systems Engineering from The George Washington University. Dr. Green earned Defense Acquisition Workforce Improvement Act (DAWIA) Level III certifications in Program Management and IT, as well as a Level III Program Management certification from the Federal Acquisition Institute (FAI). He is also a member of the Defense Acquisition Corps.

## Q: What should agency employees know about you? What attracted you to this job?

**A:** Growing up, I have always been fascinated by creativity and the critical thinking process to develop innovative solutions to solve complex problems. Once I discovered the agility that IT provided, I naturally gravitated toward this profession. However, I still believe the best IT people are the ones who truly understand the mission and strategic outcomes and know how to furnish tools and mechanisms to enable it. It sounds easy, but many times it's not — yet this is how you bring value to any organization. Additionally, I value teamwork.

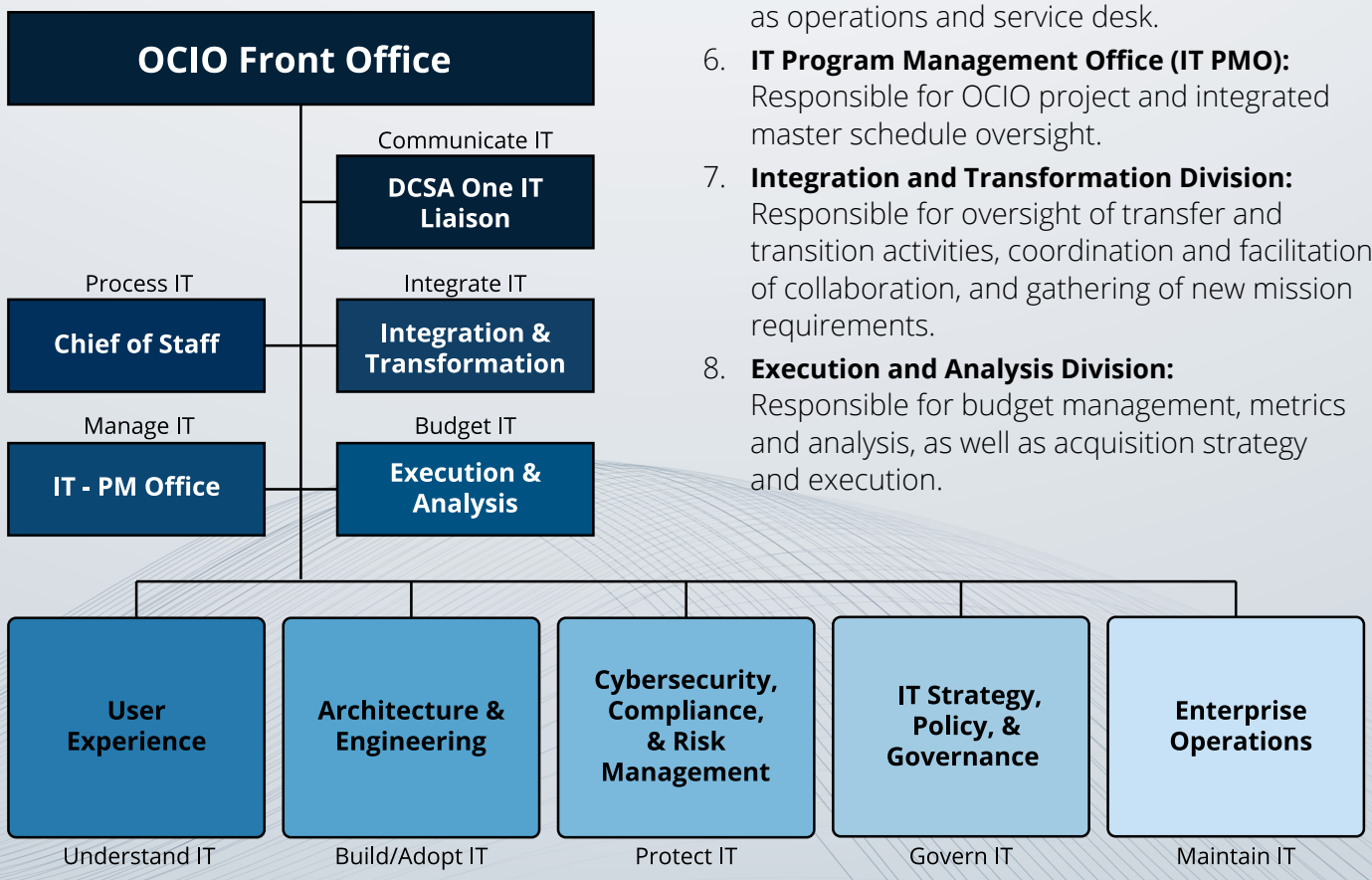
## Q: What are the biggest challenges facing Office of the Chief Information Officer (OCIO)?

**A:** As if COVID-19 was not enough, it hit amid our migration of thousands of users into DCSA. Aside from responding to that influence on OCIO's IT responsibilities, we have been balancing differing requirements and perspectives, a diverse mix of regulations, and strategic partnerships external to DCSA. Collaboration and communication will always be an essential responsibility. These responsibilities are simply part of the job, and OCIO can only strive to continuously deliver, learn, and adjust as user needs and DCSA's mission evolve over time. We take a view that hindsight is our best teacher. We will continue to acknowledge lessons from the past to inform the foresight required for IT effectiveness and to help our OCIO team grow and thrive.

## Q: I'm sure most employees don't know everything Office of the Chief Information Officer (OCIO) is responsible for. Can you give us an overview of the OCIO?

**A:** First of all, thank you for the questions and interest in the OCIO. The OCIO leads the DCSA information enterprise by defining a shared vision, setting and enforcing agency policy, and driving the standard for the information infrastructure that supports security oversight and education missions. DCSA is undergoing dramatic shifts due to the size and breadth of its workforce, the growing range of our requirements, and the availability and integration of new and exciting technological capabilities. OCIO is responsible for ensuring that current and migrating employees serving the DCSA mission across the globe have the tools, capabilities, and access to the data, systems, and applications to fulfill the agency mission. Our vision is reflected in an aspiration called "DCSA One." It speaks to OCIO's ability to provide DCSA employees with one email, on a single network, working in a single environment. The OCIO is organized into eight divisions:

1. **User Experience Division (UX):** Responsible for customer experience, relationship management, strategic communications, IT requirements, and mapping of the customer journey.
2. **Architecture and Engineering Division (A&E):** Responsible for enterprise architecture, engineering, as well as IT modernization.
3. **Cybersecurity, Compliance, Risk Management Division (CCRM):** Responsible for cyber compliance and public key infrastructure, cyber assurance management, cyber workforce compliance, and cyber defense operations.
4. **IT Strategy, Policy, Governance Division (IT SPG):** Responsible for IT governance and service delivery, IT policy and strategic management, as well as performance metrics and analysis.
5. **Enterprise Operations Division:** Responsible for network services, unified communications, infrastructure, and applications services as well as operations and service desk.
6. **IT Program Management Office (IT PMO):** Responsible for OCIO project and integrated master schedule oversight.
7. **Integration and Transformation Division:** Responsible for oversight of transfer and transition activities, coordination and facilitation of collaboration, and gathering of new mission requirements.
8. **Execution and Analysis Division:** Responsible for budget management, metrics and analysis, as well as acquisition strategy and execution.



## Q: What successes have you seen since arriving at DCSA?

**A:** I arrived during the COVID-19 pandemic. While there have been obvious impacts and implications for us all, DCSA has continued its mission unabated. OCIO's ability to pivot and apply technology in agile and nimble ways has steadfastly kept DCSA on track. Some of the pivots we've made include delivering collaboration and productivity tools to support telework, expanding Virtual Private Network (VPN) capacity from 2,000 to 8,000 users over a three-month period, and successfully migrating and onboarding legacy users. I am particularly proud of the last point, reflected in our launch of an onboarding dashboard for new hires, publication of more than 100 "how to" self-service articles, and delivery of 34 unique dashboards to allow real-time visibility into ticket trends and performance. All of this is knit together by communication, planning, policy, governance, and strategy embodied in our DCSA One IT vision and strategy.

## Q: The OCIO response was critical during COVID-19 and the push to telework. What did OCIO learn during the process? What went well, or what could have gone better?

**A:** OCIO's strong partnership with policy makers has helped to drive a successful balance between access and security. In the past year, a catalog of secure collaboration and communication tools were rolled out across the enterprise. Going forward, network bandwidth is being increased to support video teleconferencing and other requirements that are part of working remotely. Further, OCIO is committed to strengthening our failover and redundancy capabilities to always ensure network connectivity. The COVID-19 pandemic highlighted new ways of working and practices that will likely become the norm. Imbued within this new norm is OCIO's pledge to support DCSA's mobile workforce. As such, DCSA has embarked on the future capability of DCSA One Desktop Anywhere. This means providing secure access to the DCSA desktop from anywhere and any approved device. DCSA is undergoing an exciting transformation in how it meets its mission, and OCIO is here to make that possible.

## Q: As such a geographically dispersed agency, what challenges does that present?

**A:** While the data and information that DCSA employees access, produce, and use is tied to a national security mission, users have expectations when it comes to getting what they need — wherever they may be working and with whatever agency-approved device they are using to do their work. It is my expectation for OCIO that a user can securely access information, collaborate, and communicate whether logging in from a DOD workstation, from their home office, or while traveling. OCIO is implementing technology, practices, and policies to enable these types of scenarios in ways consistent with what a user would experience using commercial systems and tools.

# DCSA EMPLOYEES WEATHER EXTREME TEMPERATURES AND SEVERE CONDITIONS

A barrage of winter storms hit the southern Plains in mid-February 2021, resulting in extreme cold temperatures, extensive power outages, loss of heat, and burst water pipes. Texas was hit particularly hard. At one point during the crisis, more than 3.5 million people across the state were left in the dark and without power.

On February 14, the Texas governor declared a state of emergency, allowing federal funds to flow for emergency support. However, the extreme weather continued with several cities experiencing record overnight-low temperatures. In Dallas, the temperature was -2 degrees Fahrenheit, the city's coldest temperature recorded since 1930.

Water lines broke in many areas and power disruptions impacted water treatment plants, forcing several cities to enact residential boil-water orders. By February 18, more than 13 million people in Texas lived in areas under boil-water orders. Many were encouraged to purchase bottled water, which led to shortages across the state. Food staples such as bread and milk were also in short supply.

Despite these hardships, DCSA employees continued to work to support the mission, but it wasn't easy.

## DARREN DENNARD

Senior Industrial Security Representative Darren Dennard, Irving Field Office, was without power for about 30 hours over the course of the winter weather. "During the Snowmageddon, the power would turn on every 5-6 hours, but only for 60 to 90 minutes at a time," he said. "It was a disruption of the mission because I couldn't get on the internet and therefore couldn't connect to the VPN."

He was able to use a generator that he bought just days before the storm to keep his heat and refrigerator running. He noted that one cleared facility in the Dallas area was working under partial power outages and "used their contract guard force to provide essentially constant surveillance of the facility with around the clock guard rounds."

"I have been in Texas for the last 58 years, and I can't recall ever having the amount of snow, the continuous below freezing temperatures, or the statewide power outages like we had in February," he continued. "I learned that generators are somewhat like insurance. I don't like paying for it, but I am sure glad I have it when I need it."

## TYRONE M. BAKER

Information Systems Security Professional Team Lead Tyrone M. Baker, Irving and San Antonio Field Offices, considers himself lucky as he didn't lose power, but noted that some cleared facilities "shut down for a few days due to the extreme cold. These facilities made requests for audit variance to shut down their systems for that time and audit upon return," he said.

## JAMES M. COUCH JR.

Having grown up in Texas and Colorado, Special Agent in Charge James M. Couch Jr., Background Investigations — West Texas Field Office, understood the need to prepare. "We had foods on hand that wouldn't require heating, winterized our outside faucets as best we could, filled water bottles for drinking, filled a bathtub of water for other needs, left our faucets at a slow drip, and had flashlights and candles at the ready," he said. "During the long, cold days, we added extra layers of clothing, closed the curtains at night to conserve heat (opened during the day to let the sun do its job), and continuously reassessed our situation."

Upon returning to work, "supervisors worked to gain accountability and assess everyone's situation," he said. "A majority of the state was experiencing critical infrastructure failures of some sort, and we were

being asked to conserve power. When power was on, I found myself frantically trying to get emails and phone calls made. I was able to reach everyone on my team and report 100% accountability."

## HEATHER LONG

Special Agent Heather Long, Background Investigations — Fort Worth Field Office, and her family also prepared for the storms by filling bathtubs with water and thawing snow to supplement it. The family huddled in the living room around a fireplace. Long's husband had luckily bought "what I initially thought was a ridiculous amount of firewood, but we ended up using almost all of it," she said.

Living on a well, the family had to use a hair dryer to thaw the well pump after the electricity returned, as well as thaw a few frozen pipes to bring water back into the house. The only damage suffered was to the pool equipment. Long realized others were not as fortunate and spent the next two days "helping others by getting them water and warm food or with damage clean up," she said.

## JASON ELMORE

"As did most, we lost power every other hour and lost water for four days. Work was intermittent, as I was trying to keep the house working and kids warm," said Counterintelligence Special Agent Jason Elmore, Irving Field Office. "I know much work did not happen that week, but I did deliver 30 cases of water to members of our church family who needed it."

"We have learned that we need to definitely have working flashlights, cases of water ready, and possibly a generator," Elmore continued. "However, this was a very rare storm that happens every few decades."

## JENNIFER NORDEN

During the first day of rolling outages, state officials realized the power situation was dire and asked people to conserve energy, noted Irving Field Office Chief Jennifer Norden. "This led to one twist we have not seen in the field office before, to my recollection. During the first two days, we used the agency's weather and safety leave guidance to authorize administrative leave if personnel could not work due to the power outages, Wi-Fi/internet outages, or other storm-related circumstances. For those who did have telework capability, we still factored in the need to conserve power and thus made decisions on granting leave relative to mission essential work."

"The field office itself was without power for nearly four days, but fortunately there was no damage to the office suite or the building," Norden continued. "However, the alarm system's communication paths were affected by the outages, causing continuous notifications from the alarm monitoring company during the course of the outage and requiring vigilance to ensure the backup systems and batteries were functioning as designed."

"For me personally, the experience will be one of those defining moments that shapes my perspective on what it means to be a field office chief. Navigating the lanes of 'people first, mission always' is a profound responsibility any day of the week, but it is further intensified in a crisis," she said.

Norden listed questions that occupied her mind: How is everyone doing? What do they need? Am I communicating enough information to our team, to my fellow supervisors and to leadership? What do I need from my leadership? Do we have any emergencies at our cleared facilities and how are the facility personnel doing? Is the physical or security integrity of our field office intact? Are our 12 government vehicles in jeopardy of damage? Who's up today or down today? Since I'm directly affected, what do I need from the regional director and what are my contingencies for continued office coverage if my situation doesn't improve soon?

"In reflection, this experience validated the need for, and active presence of, effective emergency plans across our area of responsibility," Norden said, noting that tornadoes and severe storms are common in the summer, while Kansas and Oklahoma typically see ice storms in the winter.

"We are fortunate to work with facility security officers and information system security managers who keep us informed of their status even under difficult circumstances and prioritize us among the many stakeholders they have to communicate with during emergencies. We recognize the storm could have had a much harsher impact on the classified programs across the area of responsibility and are relieved that the reported impact to people and security programs was not worse," she concluded.

# BACKGROUND INVESTIGATIONS PROVIDES VETTING SUPPORT FOR THE UNACCOMPANIED REFUGEE MINORS PROGRAM

**By DCSA Background Investigations Field Operations**

In late March 2021, as the volume of unaccompanied children increased at the U.S. southern border, the Department of Health and Human Services (HHS) and U.S. Public Health Service (USPHS) needed large numbers of volunteers to provide care as part of the Unaccompanied Refugee Minors Program (URM).

To fill this urgent need, HHS quickly called on federal employees to volunteer, but these volunteers would need additional child care security checks before they could provide support. The Special Agency Checks (SACs) for child care required to support this operation fall under personnel vetting oversight of the Suitability Executive Agent (the director of the Office of Personnel Management) and within the DCSA Background Investigations (BI) mission. These checks can vary in complexity due to individual state requirements such as the submission of fingerprint cards, specific state releases, and the use of third-party vendors.

The Child Care SAC is used to satisfy the requirements of the Crime Control Act of 1990, which requires a statewide criminal history record check for a subject's current and prior states of residence. The Crime Control Act requires that these state criminal history checks be conducted for all employees and contractors that will have direct contact with children under the age of 18.

Under normal circumstances, customer agencies would collect the required information and fingerprints, and submit them to DCSA as part of a background investigation. Because these volunteers were needed quickly, DCSA needed to provide a more streamlined process to expedite the onboarding of volunteers.

DCSA BI Field Operations, with the support of the BI Customer and Stakeholder Engagement (CSE) team, surged background investigations resources and quickly established an on-site presence in Dallas, Texas, to help agencies collect the required forms and fingerprints.

Within three days of the request for assistance, DCSA BI identified six volunteers from BI Field Operations and stood up its operations at the Kay Bailey Hutchison Convention Center, in concert with HHS and USPHS.

While BI Field Operations had the lead on standing up and manning the Dallas Operations Center, DCSA solicited additional support from CSE and the Federal Investigative Records Enterprise (FIRE) to teach the agents how to roll fingerprints, access shared portals primarily used by customer agencies, and initiate investigations. The team ramped up immediately to essentially operate as an "on-site submitting agency" on behalf of HHS, even providing overnight support for operations, as needed.

However, the coordination of logistics and setup of the operations were not without their challenges. The team had to overcome multiple space and location changes as well as difficulties acquiring supplies. Nevertheless, the DCSA team remained agile and steadfastly focused on the mission, ensuring that any hiccups or road bumps did not impact the role they were playing in this humanitarian effort.

As the need for vetted volunteers grew and operations expanded into overnight shifts, BI CSE reinforcements skilled in fingerprinting arrived a few days after the initial operations standup to expand the team and provide additional support.

The entire BI team established an initial process and quickly adjusted to challenges as they arose, including moving to a formal, off-site personnel mobility center (PMC), where volunteers were fully processed. They also made adjustments based on lessons learned along the way, increasing efficiencies in the process. Additionally, the on-site agents leveraged any downtime or lulls in volunteer arrivals to process their normal case assignment work — unrelated to the HHS/USPHS operations — thereby further maximizing their efficiency and productivity.

The team worked closely with USPHS to ensure the BI Field Operations were included in all planning efforts, while continuing to coordinate and adjust their own plans for operations. This close coordination and continued interagency engagement led to the Child Care SAC station being included on the PMC checklist as a mandatory item. Each child care volunteer must adhere to and complete the mandatory items on the checklist, so having the DCSA station noted as a mandatory item exemplified the importance of the operations being conducted.

*Continued on pg. 12*

**BI FIELD OPERATIONS TEAM MEMBERS (ON-SITE SUPPORT):**

Assistant Regional Director Robert (Bob) Dubek

Special Agent in Charge Lilly Cranor

Special Agent Matt Ellis

Special Agent Donna Garcia

Special Agent Tymon Kapelski

Special Agent Heather Long

**BI CSE TEAM MEMBERS (ON-SITE SUPPORT):**

Patrick McCurdy

Keith Phillips

**BI FIRE TEAM MEMBERS (REMOTE SUPPORT):**

Janeen Beatty

Sean Bernardi

Kelli Covert

Adam Fox

Melanie Hilliard

Travis Mathers

Sherry Overly

Jennifer Phillips

Jennifer Plyler

Emmalee Schattauer

Mark Swartfager

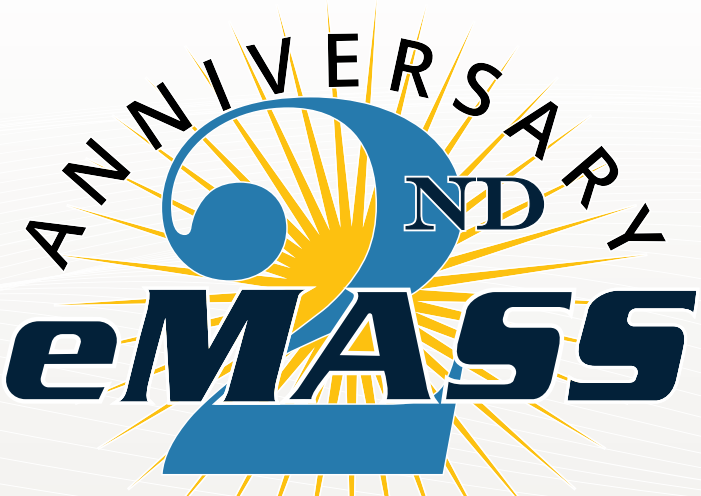
"I was really impressed how multiple independent agencies really came together, under short deadlines, supporting different pieces of a common mission, to create an outstanding personnel mobility center. Mission success is achievable thanks to solid processes in place supported by a strong team"

*— BI Assistant Regional Director Bob Dubek*

No operation like this is without challenges, but because the DCSA team had the critical fundamentals of leadership, empowerment, diversity, teamwork, and communication in place, they were able to overcome obstacles and achieve mission success. DCSA processed the 1,000th person at 11:52 a.m. on April 29, 2021. As of May 12, the team has processed 2,200 volunteer personnel for HHS.

Figure1: BI Field Operations resources processing volunteers. Middle tables: Special Agent Donna Garcia and Special Agent-in-Charge Lilly Cranor; Outside tables: Conducting fingerprinting: Special Agent Matt Ellis and Special Agent Tymon Kapelski..

Figure 2: Dry run of operational setup. From left to right: HHS local volunteer, Special Agent Matt Ellis, Special Agent Tymon Kapelski, Commander Klotzbeucher (Officer-in-Charge, PMC; O-5, USPHS), Special Agent Donna Garcia, and Special Agent-in-Charge Lilly Cranor.




# NISP eMASS CELEBRATES ITS SECOND ANNIVERSARY

The National Industrial Security Program (NISP) Enterprise Mission Assurance Support Service (eMASS) is the official database of record for government Assessment and Authorization (A&A) determinations of classified systems under the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), a common set of guidelines and minimum requirements for classified information systems. On May 6, 2021, eMASS officially celebrated its second anniversary in operation.

This anniversary comes as NISP eMASS reports 1,502 eMASS containers, 3,700 users, and 6,292 systems, with numbers continuing to grow every day. It maintains its impact due to the relationships built by DCSA information systems security professionals and team leads, who work daily with both government and cleared industry users.

Additionally, a strong partnership with the Defense Information Systems Agency (DISA) enabled the NISP Authorization Office (NAO) eMASS team to create efficiencies by publishing user guidelines, deploying updates efficiently, and evaluating how to bring new partners onto the eMASS application.

***"May 6 celebrates another successful year for NISP eMASS."***

***— David Scott, NISP Authorizing Official***

"Working closely with DISA on system enhancements, our relationships have resulted in several upgrades, including a future deployment that will reflect the significant implementation of NIST 800-53, revision 5. At the same time, we continue training our field team and providing tailored solutions which closely match our users evolving needs," he said.

The NAO appreciates the continued efforts and support of its cleared industry and government partners. Without their cooperation and dedication, this milestone would not be possible.

Serving 3,700 users and more than 6,292 systems, the NISP eMASS is one of the largest in the nation.

# DISS TAKES THE HELM AS SYSTEM OF RECORD FOR PERSONNEL SECURITY

The Defense Information System for Security (DISS) officially replaced the Joint Personnel Adjudication System (JPAS) as the system of record (SOR) for Department of Defense personnel security management on March 31, 2021.

DCSA played an integral role in the final stages of DISS delivery, assuming responsibility for the IT system from the Defense Manpower Data Center (DMDC) on October 1, 2020. To prepare for the transition, DCSA worked with customers to ensure they understood the transition steps and had the resources they needed to use DISS proficiently. DCSA subject matter experts delivered eight publicly available trainings in partnership with NCMS, the Society of Industrial Security Professionals, to help prepare more than 50,000 system users for the transition.

DCSA also worked with users to ensure all JPAS capabilities were fully available in DISS, deploying four capability releases to meet or exceed JPAS functionality before the transition date and continues to offer release updates with additional features.

"Changes to defense information systems are massive undertakings," acknowledged DCSA Director William K. Lietzau. "This change impacted the entire enterprise — DOD military, civilians, and contractors. I am incredibly proud of the DCSA team members who worked diligently to ensure as smooth a transition as possible."

DISS will be an integral step toward the National Background Investigation Services (NBIS) platform currently in development. As the new personnel vetting IT system that will transform the background investigation process, NBIS will deliver stronger security, faster processing, and better information sharing, while also enhancing user experience for government users, industry, and applicants. It is the future of personnel vetting, enabling the federal government to meet necessary Trusted Workforce 2.0 policy reforms.

"Bringing DISS over to DCSA was unquestionably the right move as we work to reform the personnel vetting process and develop the NBIS toolbox," said Jeff Smith, NBIS executive program manager. "This team worked very hard to finalize the DISS system, and we are continuing to fine tune it this quarter."

## WHAT IS DISS?

DISS is an enterprise-wide personnel vetting case management system for national security eligibility, suitability, fitness, and credentialing decisions for DOD military, civilian, and contractors. DISS provides secure communications between adjudicators, security officers, and components, allowing users to request, record, document, and identify personnel security actions. DISS provides real-time information regarding clearance, access, and investigative status to authorized personnel, allowing users to process visit requests and report security incidents. It is comprised of the Case Adjudication Tracking System (CATS), the Joint Verification System (JVS), and Appeals.

## DISS COMPONENTS

### Case Adjudication Tracking System (CATS)

Performs electronic and human adjudication functions, automating record-keeping for security clearances, HSPD-12, military fitness, and suitability determinations.

### Joint Verification System (JVS)

Enables DOD professionals to document security clearance access and verify eligibility determinations.

### Appeals

Supports the Defense Office of Hearings and Appeals (DOHA) and the Personnel Security Appeals Board (PSAB) with completing due process for subjects appealing adjudicative determinations.

## DISS BENEFITS & THE FUTURE OF PERSONNEL VETTING

DISS provides numerous enhancements over JPAS, including better adjudication workflow management, e-delivery of investigation results, electronic storage of background investigation files, e-adjudication of cases containing no disqualifying information, and enhanced security management capabilities.

- **Enterprise-wide solution.** A single, integrated solution enables interagency standards, communication, and reciprocity.
- **Accelerated workflows.** DISS integrates workflows between adjudicators and security management offices to streamline personnel security actions, information, and timelines.
- **Electronic adjudications.** E-adjudication shortens timelines and redirects resources to address higher risk or higher priority investigations.
- **Enhanced user experience.** Users now have visibility over the entire case inventory and end-to-end status monitoring in a single platform.
- **Secure document exchange.** DISS provides the ability to securely submit and receive documents, including the Classified Information Nondisclosure Agreement (Standard Form 312).

## DISS RESOURCES

For more information on DISS, system operating status, and training tools, visit the DCSA website at www.dcsa.mil/is/diss. End users can also reach out to the DCSA Contact Center for assistance at dcsa.ncr.nbis.mbx.contact-center@mail.mil

# HISTORY OF JPAS

**2001**

JPAS was created from the U.S. Air Force Sentinel Key program that originally started in October 1998. At one point, JPAS had over 104,000 active users and averaged over 2,000 concurrent users at peak times.

**2004**

JPAS became the system of record for DOD. Industry use of JPAS enabled DOD to move resources previously used to update contractor clearance records to other efforts, including adjudication of contractor clearances.

**2008**

DOD initiates development of a replacement for JPAS.

**2020**

DCSA was authorized by USD(I&S) to direct the Military Departments, the OSD and DOD Components, and National Industrial Security Program (NISP) contractors under DOD security cognizance to use DISS.

Users were transferred from JPAS to DISS as the required functionality became available and passed user acceptance testing.

**2021**

JPAS entered a "Read Only" status to allow users time for final data

# CONTINUOUS VETTING PROVIDES AN ENHANCED RISK-MANAGEMENT APPROACH FOR EARLY ISSUE DETECTION

**By Heather Mardaga and Zaakia Bailey**
**Vetting Risk Operations**

Continuous Vetting (CV) is the real-time review of an individual's background, at any time, to determine if they continue to meet the requirements to uphold the eligibility to access classified information. An individual is defined as someone who has DOD affiliation(s), eligibility for access, and a signed SF-86 dated 2010 or later. This process relies on a combination of automated record checks, agency specific information, and self-reported information to create an enhanced risk-management approach that facilitates early detection of issues.

Unlike previous automated record checks, often referred to as Continuous Evaluation (CE), CV will replace the five-and-10-year periodic reviews with ongoing, and often automated, determinations of a person's security risk in 2022. CV incorporates automated record checks expanded from CE, pulling information from government and commercial data sources. When DCSA receives an alert, it assesses whether the alert is valid and worthy of further investigation and adjudication. Addressing potential indicators early allows individuals the opportunity to seek assistance and mitigate triggers before they become an insider threat.

## HOW CV WORKS:

John Doe, a cleared contractor, was recently arrested for driving under the influence (DUI), which is considered derogatory information under the Alcohol Consumption and Criminal Conduct adjudicative guidelines. Because he has been enrolled in CV, an alert will be generated via automated record checks.

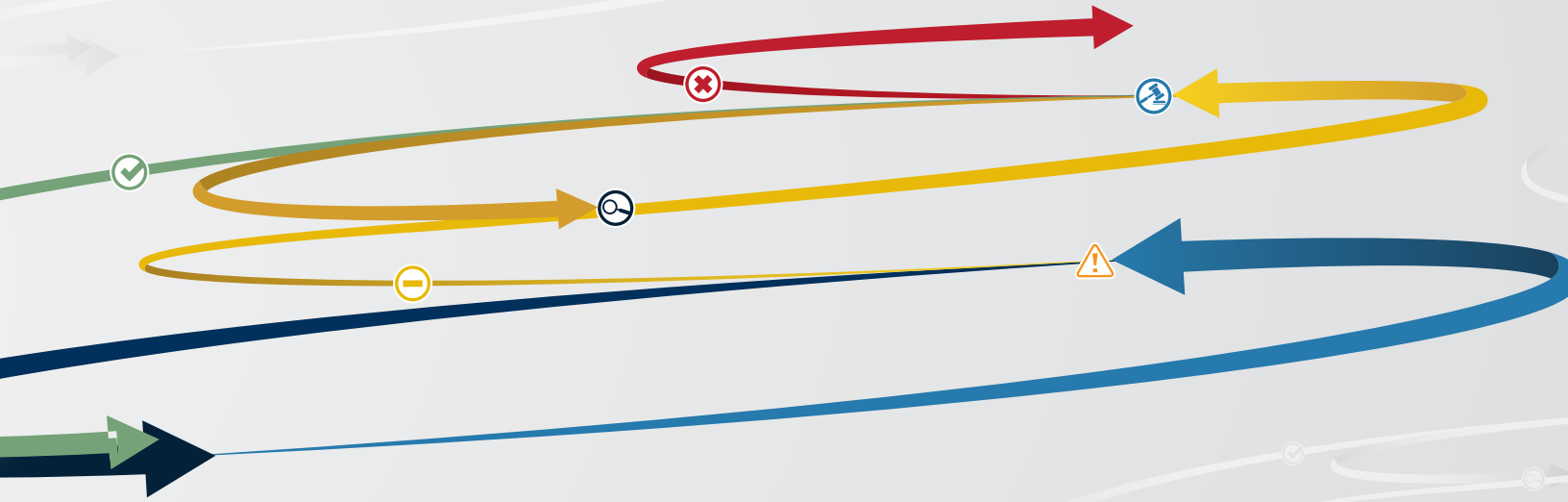
When DCSA receives the CV alert, the first action is to confirm that the alert belongs to the individual, using personally identifiable information and open source searches as needed.

The second step is to determine if the information was reported. Did John Doe report the DUI arrest to his security manager or facility security officer (FSO) as required? If the individual did not report, the information will be provided to the security manager or FSO through an incident report, with a request for additional information.

The security manager or FSO can then address the issue with John Doe, providing the opportunity to help John Doe seek treatment and mitigate the security concern associated with the arrest. They can also provide information that assists in the adjudication of the incident.

The incident report and any provided information is forwarded for adjudication to assess the whole person, i.e., Did John Doe have a history of alcohol issues, DUIs, or arrests before this or is this an isolated incident? ?

The goal of CV is to identify security-relevant issues in real-time to enable an individual the opportunity to mitigate the issue before it becomes an insider threat concern. Or, in situations where insider threat indicators are already present, CV ensures classified information remains protected, while conducting the appropriate investigation to collect the facts and make the appropriate adjudication of the issue.



When executed, CV is capable of providing critical intervention to a cleared employee six to seven years before the traditional background investigation intervals. Timely identification, reporting, and investigation (when necessary) of security-relevant concerns is just as critical to protecting national security as it is to help the cleared individuals who help preserve mission readiness.

**To help understand what CV is and what it will become, here are some common myths and facts:**

**MYTH:** CV is only automated record checks.

**FACT:** CV is more than automated record checks. It includes agency specific information, self-reported information, and data collected by other sources to use risk indicators to determine the appropriate time to conduct a background investigation.

**MYTH:** With CV, cleared individuals do not need to report security-relevant changes.

**FACT:** All cleared government personnel are required to self-report security-relevant information per Security Executive Agent Directive (SEAD) 3. Industry will soon receive guidance explaining how SEAD 3 will be implemented for cleared industry in an upcoming Industrial Security Letter.

***For more information on CV, continue to monitor the DCSA website for updates and Center for Development of Security Excellence (CDSE) for a personnel security toolkit.***

**MYTH:** CV and CE are the same thing.

**FACT:** CV encompasses much more than CE. CE only utilized automated record checks to identify security-relevant issues, while CV utilizes a myriad of data sources to determine when a security-relevant issue exists in an individual's background.

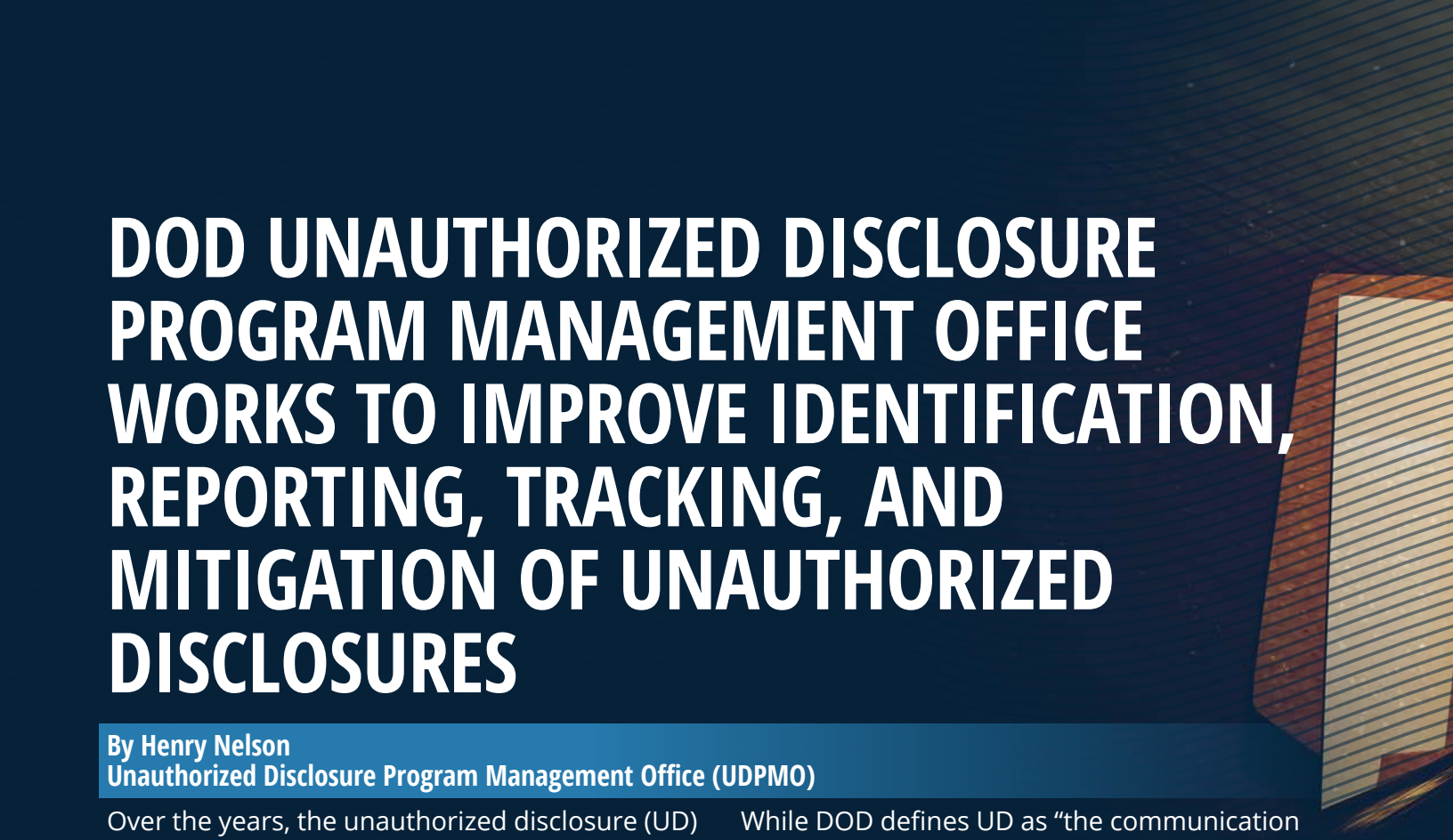
**MYTH:** CV only applies to the Department of Defense (DOD).

**FACT:** The Executive Correspondence issued by the Security Executive Agent (Office of the Director of National Intelligence) and the Suitability & Credentialing Executive Agent (Office of Personnel Management) in January 2021 provided critical guidance to all federal agencies on how to begin implementing mandatory personnel vetting reforms under the Trusted Workforce (TW) 2.0 initiative. DCSA is responsible for creating a CV-compliant program for DOD, and contractors under the National Industrial Security Program (NISP). DCSA also offers CV as a service to other federal agencies, which may leverage DCSA's intermediary TW 1.25 services to meet the requirement of having its cleared population enrolled in a CV-compliant security program by the end of fiscal year 2021.

**MYTH:** CV only applies to security managers and FSOs.

**FACT:** Everyone has a role in CV. While security managers and FSOs play a major role, there are several others who also provide key inputs into CV: supervisors, human resources, insider threat officials, information technology monitoring, and government referrals.

# DOD UNAUTHORIZED DISCLOSURE PROGRAM MANAGEMENT OFFICE WORKS TO IMPROVE IDENTIFICATION, REPORTING, TRACKING, AND MITIGATION OF UNAUTHORIZED DISCLOSURES



**By Henry Nelson**
**Unauthorized Disclosure Program Management Office (UDPMO)**

Over the years, the unauthorized disclosure (UD) of classified national security information (CNSI) and controlled unclassified information (CUI) has undermined U.S. foreign policy and weakened our government's ability to protect the security of the nation against its adversaries.

As UDs are viewed as an "insider" threat, in December 2016, the Department of Defense (DOD) Unauthorized Disclosure Program Management Office (UDPMO) was realigned from Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) to the DOD Insider Threat Management and Analysis Center (DITMAC) within DCSA. This move would more closely align UDPMO with the DOD Insider Threat enterprise. UDPMO is recognized as a unique mission within the DITMAC, aligning to both information security and insider threat policies. It provides DOD an enterprise-level management and operational capability to improve identification, reporting, tracking, and mitigation of UDs.

While DOD defines UD as "the communication or physical transfer of classified or CUI to an unauthorized recipient," not all UDs need to be reported to UDPMO. The UDPMO should be notified of:

1. **All incidents involving the release of CNSI and CUI in the public domain.**
2. **The release and/or enabled theft of information relating to any defense operation, system, or technology determined to be CNSI or CUI.**
3. **Information wherein an individual disclosed classified information and/or CUI to unauthorized person or persons resulting in administrative action, referral for criminal and/or counterintelligence investigation, and/or resulted in the suspension or revocation of a security clearance.**

When UDPMO receives a confirmed report of UD in the public domain (podcast, print articles, internet-based articles, books, journals, speeches, television broadcasts, blogs, or postings), it submits a UD referral to the Department of Justice (DOJ). The referral includes findings from a preliminary inquiry conducted by the affected component, a damage/impact assessment, and a media leaks questionnaire for those UDs appearing in the media.

This process was exercised in the case of Henry Kyle Frese, a former Defense Intelligence Agency (DIA) employee who pled guilty to the willful transmission of Top Secret national defense information to two journalists in 2018 and 2019. As a result of Frese's actions, he was sentenced to 30 months in prison on June 18, 2020.

"Frese violated the trust placed in him by the American people when he disclosed sensitive national security information for personal gain," said Assistant Attorney General for National Security John C. Demers in a DOJ statement. "He alerted our country's adversaries to sensitive national defense information, putting the nation's security at risk. The government takes these breaches seriously and will use all the resources at our disposal to apprehend and prosecute those who jeopardize the safety of this country and its citizens."

The Frese case, like others, should serve as reminder to all DOD civilians, contractors, and military personnel of their lifelong responsibility to protect and safeguard information. This applies while the individual is actively employed with the U.S. government and continues when the individual retires or leaves government service. Individuals may use the Whistleblower Protection Enhancement Act (WPEA) to report information they reasonably believe provides evidence of a violation of any law, rule, or regulation, gross mismanagement, a gross waste of funds, abuse of authority, or a substantial danger to public health and safety.

# BACKGROUND INVESTIGATIONS PLAYS ROLE IN INSIDER THREAT IDENTIFICATION

**By Saoirse Spain**
**Background Investigations Directorate**

**The following BI employees also contributed to this article:** Janeen Beatty, Federal Investigative Records Enterprise; James Cratty, Quality Oversight; Ryan English, Centralized Investigations; Jeffrey Fitzpatrick, International Activity; Christina Johnson, Quality Oversight; Jon Maffet, Customer & Stakeholder Engagement

The federal workforce is trusted to protect and defend national security, and establishing a baseline of trust in the workforce on the front end of their service is critical. DCSA's Background Investigations (BI), as the federal government's primary investigative service provider, plays an important role in establishing that trust and is part of the first line of defense against insider threats. The BI mission efficiently and effectively investigates and develops critical information that federal agencies use to make determinations on their specific populations.

BI conducts more than two million background investigations annually for 100+ federal agencies, which accounts for 95% of the federal government. The team works to collect, review, oversee, and analyze investigative findings to produce investigations that customer agencies rely upon to make trust determinations. It is the goal of the BI mission to investigate, collect, develop, and report all relevant information needed to make informed decisions concerning the eligibility, access, and suitability of the workforce.

BI's multi-source products and comprehensive information collection is unique and a great repository for not only its customer agencies, but also for partner agencies who protect national security. Background investigations identify behaviors, traits, and other patterns and factors that could either pose a threat to national security or conflict with a person's suitability or fitness for government work. DCSA's background investigations are often the first and most comprehensive source of information to establish a baseline enabling the government to identify potential insider threat indicators, and detecting these indicators can prevent human threats from entering the federal government's ecosystem. DCSA BI has long-established relationships with customer agency security representatives and insider threat hubs to share information and assist in detecting, deterring, and mitigating insider threats allowing agencies to comply with insider threat mandates, such as Executive Order 13587.

The BI mission coordinates internally, with its customers, and with other government agencies to complete its investigations. Additionally, through this coordination, the BI mission also provides advance notifications about serious issues to customer agencies, and these notifications allow customers an opportunity to address the threat as the background investigation continues toward completion. This combination of investigation, coordination, and collaboration creates a structure dedicated to short-circuiting the immediate threat to the federal workforce.

The BI mission encompasses many specialized offices and teams, which contribute to a full insider threat picture.

## Customer & Stakeholder Engagement (CSE)

CSE is the primary customer agency interface and assists the threat offices with joint personnel security duties by supporting customers who have insider threat questions related to the investigative process. CSE's Agency Liaisons play a vital role in sharing information between customers and the BI Mission to ensure all parties are kept apprised of important insider threat updates specifically related to the background investigative process.

## BI Field Operations

Field Operations is comprised of a hybrid model of both federal and contract investigators located across the U.S., completing work at home and abroad. These investigators conduct hundreds of thousands of interviews and record searches annually. Field Operations plays a critical role in supporting national security threat evaluation by identifying and reporting — in real time — a myriad of issues, concerns, and threats to support initial and continued suitability, security and credentialing decisions made by more than 105 departments and agencies. The BI Mission Field Operations includes teams that identify high risk, manage priority, and sensitive background investigations. Together, these teams provide direct case management that assists in developing and coordinating serious concerns associated with loyalty, terrorism, foreign influence, aggravated criminal, and insider threat issues. Leadership and analysts within Field Operations also produce reports and specialized products to keep senior leadership and our customer agencies informed about serious concerns and possible threats identified during the BI process that impact the trusted federal workforce.

## Federal Investigative Records Enterprise (FIRE)

FIRE supports the DCSA mission by requesting, processing, conducting, analyzing, and reporting the results of investigative records for the DCSA BI mission. Throughout this process, FIRE is the first line of defense in identifying and flagging potential derogatory information that could be considered national security, public trust, or insider threat information. Over 25 million records are obtained annually from federal, state, local, and vendor data repositories — including National Agency Checks and law checks. FIRE is also responsible for performing the end-to-end case processing functions for the BI mission. FIRE maintains the critical relationships and agreements with federal, state, local, and vendor data sources, and promotes process efficiencies and records automation with data source partners. In this way, FIRE enables the BI mission to collect data from a variety of sources to begin establishing the "whole-person" concept for the investigation.

## Quality Oversight (QO)

In addition to ensuring investigative products conform to federal investigative and quality assessment standards, QO also generates criminal referrals, identifies and refers serious threat indicators reported in background investigations conducted by DCSA for further analysis and investigation, and informs agencies of serious security issues that have developed over the course of the investigation. QO also oversees Reimbursable Suitability/Security Investigations (RSIs), an integral component to insider threat mitigation. The RSI is a tailored investigative product distinct from tiered investigations that enables agencies to request specific and focused investigative activities to resolve a variety of issues, including those representing insider threat indicators.

BI's specialized teams work diligently every day applying their expertise to ensure comprehensive, critical information is captured and shared with stakeholders in a timely manner, thereby enabling their decision making and hopefully preventing bad actors from entering or remaining in the federal workforce. This essential role that BI plays in national security and the insider threat prevention landscape cannot be undervalued. By assisting customers in detecting, deterring, and mitigating insider threats, BI aids in identifying and preventing potential threats.

# MOVEMENT OF CLASSIFIED INFORMATION BETWEEN U.S. AND FOREIGN GOVERNMENTS

**By Richard Stahl**
**Critical Technology Protection (CTP)**

After World War II, the United States government authorized exports of defense technology to preserve national security, expand foreign policy, and build the economy through foreign commerce. Since then, the United States has opened our export doors even wider, allowing increasing amounts of high technology beyond our borders.

The expansion of technology exports with international programs has a two-fold effect. First, it increases the nation's industrial base by bringing in funds and ideas that support the economy. However, it also creates foreign competitors of the same products and procedures being exported. Although technology sharing brings allies closer together in terms of military defense, it also increases the opportunity for technology compromises, in turn, jeopardizing national security.

An international program is a lawful and authorized effort in which there is a contributing or receiving foreign participant, and information is transferred from one country to another. It can be categorized as commercial or government. Commercial transfers involve direct commercial sales (DCS), usually initiated by a U.S. contractor to sell controlled defense articles or services. Government transfers involve foreign military sales (FMS), in which the U.S. government sells a defense product to a foreign government. Both types of sales require strict adherence to security protocols for the protection of classified information.

The International Branch of the International and Special Programs Division within CTP provides security and administrative oversight of DCS and certain FMS exports by U.S. defense contractors to foreign governments and foreign contractors. This includes permanent and temporary imports of classified information in compliance with security agreements.

The approval process for shipments can be very complex and time consuming. A plan for one shipment can exceed 50 pages, covering every detail along the way, including identification of the carrier, the countries of transit, any approved licenses, etc. The branch then coordinates (or sometimes negotiates) with our counterparts in foreign governments, and in transit countries the item might travel through, to reach consensus and subsequent approval. This process can range from a week to four weeks per plan.

DCSA has a legal obligation to directly support bilateral agreements between the United States and foreign partners to ensure shipments are completed in a timely and lawful manner. For perspective, the branch coordinates and approves approximately two shipments of classified information each day. There has been a 25% increase in shipments over the past three years, with 370 shipments in 2019, 460 in 2020, and we are on pace to approve 572 in 2021.

Additionally, the International Branch represents DCSA in international matters, such as meetings, conferences, and visits to other countries conducted under the National Disclosure Policy Committee (NDPC). The branch also supports the negotiation of international industrial security arrangements with other governments and plays a key role as a liaison to foreign government security officials, other government organizations, and corporate international offices. This liaison forms the framework for key functions, including:

- **Establishing government-to-government channels for subsequent exchanges of assurances.**
- **Approving security arrangements (i.e., hand carriage plans and transportation plans approvals) on behalf of the United States and coordinating these approvals with foreign governments and NATO.**
- **Requesting classification guidance and evaluating compromise reports involving foreign government or NATO information and providing notification to the originating foreign governments.**

By conducting the coordination, approval, and oversight for the movement of classified information between the United States and over 68 foreign governments, the International Branch helps the U.S. comply with international laws, treaties, and uphold bilateral agreements.

# DCSA PLANS OVERSIGHT OF CONTROLLED UNCLASSIFIED INFORMATION PROGRAM FOR NISP CONTRACTORS

**By Clement LaShomb, Richard Rayner, Lilian Benitez, and Dahlia Thomas**
**Critical Technology Protection**

In 2010, Executive Order 13556 established the Controlled Unclassified Information (CUI) Program. CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable laws, regulations, and government-wide policies, but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

The CUI program intends to establish open and uniform processes for managing information that requires these safeguards or dissemination controls, and it replaces several markings that are used to protect information, including "For Official Use Only" or FOUO, "Sensitive but Unclassified" or SBU, and "Law Enforcement Sensitive" or LES, as well as others.

## CUI IN NATIONAL SECURITY

The loss of aggregated CUI poses a significant risk to national security. The Department of Commerce and FBI estimate over $600 billion in annual losses related to this information. The majority of the loss happens on unclassified systems without stringent safeguards and security controls that are typically found in the classified domain.

## DCSA'S CUI RESPONSIBILITIES

DOD Instruction 5200.48, "Controlled Unclassified Information," assigns responsibilities to the DCSA director to administer the DOD CUI Program for contractually established CUI requirements for contractors in classified contracts. Responsibilities also include:

- Administering the DOD CUI Program for contractually established CUI requirements for contractors in classified contracts.
- Assessing contractor compliance with contractually established CUI system requirements in DOD classified contracts associated with the NISP.
- Establishing a process to notify the DOD CIO, USD(R&E), and USD(A&S) of threats related to CUI.
- Providing security education, training, and awareness on the required topics identified in Section 2002.30 of 32 CFR.
- Providing security assistance and guidance to the DOD Components on the protection of CUI.
- Serving as the DOD-lead to report unauthorized disclosure of CUI.
- Coordinating with the DOD CIO to implement uniform security requirements for NISP contractors.
- Consolidating DOD Component input on the oversight of CUI protection requirements in DOD classified contracts for NISP contractors.

DCSA's Critical Technology Protection Directorate is currently establishing functional capabilities to administer and manage the agency's CUI responsibilities outlined in DODI 5200.48. To date, personnel supporting this effort have engaged with government and industry stakeholders and internal DCSA elements, including the Center for Development

*"The loss of classified and controlled unclassified information is putting the Department's investments at risk and eroding the lethality and survivability of our forces."*

— Former Secretary of Defense James Mattis, October 24, 2018

of Security Excellence (CDSE). DCSA is exploring all options with respect to how it will administer its CUI responsibilities, including information sharing agreements with other agencies within the CUI domain and leveraging artificial intelligence and machine learning capabilities. DCSA's goal is to reach an initial level of implementation of its CUI responsibilities by October 1, 2021.

## WHAT CAN INDUSTRY DO NOW?

Until DCSA reaches initial implementation, there are many steps industry can take in the interim. This includes reviewing existing contracts and engaging with government customers to determine which, if any, CUI requirements are applicable to current contracts.

Industry is encouraged to review CUI resources and training available on the Center for Development of Security Excellence (CDSE) website to include the CUI toolkit and "DOD Mandatory Controlled Unclassified Information (CUI) Training for Contractors (IF141.06.FY21.CTR)" course. The CUI toolkit includes training, policy documents, resources, and a frequently asked questions video, which CDSE has made available at: www.cdse.edu/toolkits/cui/index.html. In addition, industry security professionals are encouraged to review the DOD CUI Registry at www.DODcui.mil to familiarize themselves with CUI organizational index groupings and CUI categories.

## CUI CATEGORIES

Categories of information constituting CUI include but are not limited to:

- **Privacy Information**
- **Critical Infrastructure**
- **Tax**
- **Export Control**
- **Law Enforcement**
- **Financial**
- **Intelligence Information**

## WHAT IS CUI?

- Intended to establish an open and uniform program for managing information that requires afeguarding or dissemination controls.
- Replaces FOUO, SBU, LES, and other labels and markings previously used.
- Categories such as privacy, tax, law enforcement, critical infrastructure, export control, financial, and intelligence information that requires special safeguarding.

## WHAT IS NOT CUI?

- Classified information or a classification.
- Corporate intellectual property (unless created for or included in requirements related to a government contract).
- Publicly available information.

# ONBOARDING EVOLVES INTO THE NEW EMPLOYEE EXPERIENCE (NEX)

**By Larry Cunningham**
**Employee and Leader Development Program**

Many DCSA employees might recall their attendance and participation at the legacy New Employee Orientation (NEO) while at the Defense Investigative Service (DIS) or Defense Security Service (DSS). Traditionally, NEO was a two-day event hosted at headquarter locations, shifting from Braddock Place in Alexandria, Virginia, to the DSS Academy in Linthicum, Maryland, and finally the Russell-Knox Building in Quantico, Virginia. Newly assigned employees were welcomed to the event and provided a notebook containing copies of the event presentations. Organizational representatives presented and discussed respective mission areas over 45- to 60-minute modules.

However, all of this has recently changed. In November 2020, the Human Capital Management Office (HCMO) launched a pilot program, the New Employee Experience (NEX).

"We originally developed NEX to be an in-person program at the DCSA headquarters in Quantico," said Dr. Fred Bolton, chief of the HCMO Employee and Leader Development (ELD) Division. "Our goal was to create an interactive training environment, using required annual and initial training as the material to support acculturation to the agency. Training sessions were developed for instructor-led delivery, using DCSA as the context for the activities with delivery by our own subject matter experts," he continued. "Unfortunately, COVID-19 intervened, and we had to shift from physical to virtual in-person delivery."

The ELD team applied an instructional systems design framework to adapt and enhance the old NEO approach. This initiative included the complete review of NEO documents, products, and services and a comprehensive review of training requirements. The final NEX product included refinement of the NEX curriculum and synchronization with the Microsoft (MS) Teams delivery platform.

Additionally, HCMO employees and other available DCSA course presenters attended a "Facilitating Virtual Training" event, delivered by the Association for Talent Development. This synchronous and asynchronous training activity introduced participants to the skills, techniques, and delivery requirements associated with developing, producing, and delivering online training sessions, all within the DCSA NEX virtual environment.

The November 2020 NEX pilot had 27 new employees in attendance, with 29 new employees at the December 2020 session, and 24 new employees at the January 2021 session. Daily feedback and after-action reviews with new employees, NEX presenters, and ELD representatives provide the ELD team an opportunity to adjust where necessary to ensure training and learning objectives are accomplished. This practice has continued with each NEX iteration, ensuring that new employees are attending a training event that is rewarding, engaging, and meeting learning objectives.

The beginning of each NEX session begins with a "start-up and systems check" to ensure participants successfully sign into MS Teams, which can be quite challenging given the diversity of individual equipment and internet service provider needs. Each day, Alex Rivera, the Leadership Development Program (LDP) manager, Dr. Bolton, and others on the ELD team navigate challenges that require rapid solutions, such as fixing connection problems.

LDP Administrator Larry Cunningham stated, "The success of the NEX experience is a direct result of two elements: Dr. Bolton and Alex Rivera knowing the capabilities and limitations of the MS Teams platform, as well as individual and organizational IT challenges, and their extensive training and higher education backgrounds in delivering such products and experiences."

The experience on day one begins with the introduction of a senior sponsor (a DCSA Senior Executive Service employee) who maintains multiple personal engagements with the NEX cohort during the course. The senior sponsor also administers the oath of office, wherein the new employees swear allegiance to "support and defend the Constitution of the United States." After serving as the senior sponsor for an iteration of the NEX, Chief of Security Programs Edward "Ned" Fish said, "The DCSA NEX is the best newcomer orientation program I have witnessed in my over 35 years of time and experience in the DOD."

Over the course of two weeks, employees participate in 40 presentations and 18 break-out sessions. Presentations are delivered by mission area representatives that introduce the new employee to the DCSA organization and culture.

Each presentation is unique in content and includes learning activities that support the ingestion and transfer of knowledge.

Each curriculum topic within the NEX includes the topic presentation, NEX participant textbooks, facilitator guides, student materials, etc. Select topics also include facilitated break-out sessions that consist of multiple learning activities (e.g., Kahoot and Jeopardy games, knowledge checks, small group discussions, reflection exercises, etc.). On the last day, participants have the opportunity to meet DCSA Director William K. Lietzau and ask questions during a one-hour scheduled engagement.

A recent participant, Lisa Greenawalt, contract representative in the Applicant Knowledge Center in Boyers, Pennsylvania, testified, "You both — and Larry too — have made my first two weeks as a federal employee very enjoyable. I have enjoyed the lessons, the jokes, and the laughs we have all got to share in. Even though I am excited to start my actual job within DCSA, I am going to miss the interactions we have had with you both. Thanks again so much for making my first two weeks really enjoyable and providing us with very valuable information that will benefit us for years to come in our federal career."

Over 50 individuals have been involved in supporting the NEX. To date, there are more than 240 lessons or events and 550 separate breakout sessions to support 225 new employees. Delivery of the virtual NEX will continue with scheduled monthly sessions until DCSA returns to full operational capability with no travel restrictions, fully open facilities, and a return to face-to-face events.

MISSION: **YOU!**
NEW EMPLOYEE EXPERIENCE

# GROWING A WORLD CLASS ACQUISITION, CONTRACTING WORKFORCE: DCSA ON TRAC!

**By Elaine Daniel**
**Acquisition and Contracting**

With today's increasingly complex federal acquisition landscape, acquisition professionals must possess deep technical knowledge and strong interpersonal skills to effectively manage current capability portfolios, drive cost-effective solutions, and creatively manage end-to-end acquisition and procurement processes.

To meet the demand for growing and sustaining top-notch talent, DCSA's Acquisition and Contracting (AQ) team created a robust professional development program called Training and Reach-Back in Acquisition and Contracting (TRAC). The TRAC program consists of three foundational levels: Student Intern Level, Entry-to-Mid Level (apprentice program), and the Journey Level and above. Along the TRAC continuum, DCSA AQ employees can participate in a variety of training and experiential development opportunities to enhance and further their acquisition careers. AQ is also sharing the TRAC model with interested DCSA partners in support of their own employee developmental efforts.

Within each TRAC level, tailored developmental plans enable staff to become more effective in their current position, prepare them for potential advancement in AQ, provide meaningful personal development challenges, and facilitate lifelong learning. Specific developmental activities and timing are determined through work planning and goal-setting discussions between an employee and their leadership team.

All TRAC levels include the following common elements:

- **Completing the Gallup CliftonStrengths Finder assessment — a tool that helps organizations move away from the command-and-control management style to create a culture that focuses on people's strengths and development — and reviewing results in the context of the employee's individual team and larger AQ office.**
- **Internal rotational opportunities (via temporary rotations or longer-term re-assignments).**
- **Mentoring/shadowing with key stakeholders, customers, and subject matter experts either within and/or outside of AQ.**
- **Workshops and brown bag learning sessions hosted both internally and externally covering a variety of topics such as price and cost analysis, Other Transaction Authority (OTAs) agreements, and much more.**
- **Regular program assessments and feedback opportunities to ensure TRAC activities and programming remain relevant to the employee's ongoing growth path.**

Unique aspects of individual TRAC levels include:

## STUDENT INTERN TRACK

The student intern track focuses on individuals who are currently enrolled in school and exploring future career possibilities. In general, the program offers a paid summer internship, providing students real-world exposure to various DCSA AQ career opportunities and the ability to contribute to the agency via short-duration projects.

In 2021, DCSA AQ is piloting the DOD College Acquisition Internship Program (DCAIP), which is a paid, 10-week summer internship providing structured mentorship and real-world exposure to Department of Defense acquisition workforce career opportunities for second- and third-year undergraduate students.

For more information about DCAIP, please see: https://www.hci.mil/DODcareers/internship.html.

## ENTRY-TO-MID LEVEL TRACK (APPRENTICE PROGRAM)

This three-to-four-year blended learning program is designed for employees who are progressing from GG-1102-07/09 to the GG-1102-12 full performance level. By the end of the apprentice program, participants complete a comprehensive development plan that includes mandatory formal coursework, on-the-job training involving multiple real-world contracting requirements, developmental rotational assignments, workshops, and mentorship. By graduation, participants will have earned their Defense Acquisition Workforce Improvement Act (DAWIA) Level 2 Certification in Contracting and completed a capstone project.

AQ's inaugural apprentice program framework includes the following key elements:

- Onboarding program with supervisor
- Customized formal training plan for completion of DAWIA courses
- Quarterly workshops/brown bag sessions conducted by the Defense Acquisition University (DAU) and AQ
- Collaborative informal peer learning and engagement with other AQ apprentices
- Developmental rotations both within AQ and external entities that may include project-based learning and on-the-job training
- Mentorship from the apprentice branch chief and other AQ leaders
- Shadowing key customers, partners, and stakeholders either within and/or outside of AQ
- Capstone project
- Program evaluation and graduation

After working with the inaugural TRAC apprentices during onboarding, AQ's Chief of Staff Charlie Meyer noted, "I was pleasantly surprised by the breadth and depth of professional experience of those joining the AQ apprentice program. In the initial cadre alone, there was a former county school superintendent, two prior practicing attorneys, and several apprentices with unique private sector contracting and program management experience. They are bringing new ideas and valuable fresh perspectives to share with DCSA as they work together to obtain their contracting certifications."

## JOURNEY LEVEL AND ABOVE TRACK

This track is a rotational program for full-time employees who are GG-13 and above. Annually, the AQ leadership team rotates up to 10 individuals to different parts of the organization to offer career broadening opportunities, fulfill goals in individual development plans, and match skillsets to appropriate work. This track also includes leadership development initiatives as AQ leverages existing DCSA leadership development programs and opportunities to supplement these efforts with customized AQ leadership development, coaching, and leadership cadres.

## PROGRESS AND PLANS

DCSA AQ successfully launched all three TRAC program components in fiscal year 2021.

- On the Student Intern track, two college students are interning with AQ this summer.
- On the Entry-to-Mid Level track, AQ created the apprentice branch, hired and onboarded nine apprentices and an apprentice branch chief, and began implementing the various developmental components of this track.
- On the Journey Level and Above track, AQ employees rotated to new assignments based on their interests and completed the DCSA Leadership Development Program (LDP). They also applied for external leadership programs, partnered across organizational lines in the Process Improvement and Workforce Engagement leadership cadres, and participated in AQ's contractor-supported organizational development and leadership coaching effort.

In the next year, AQ plans to refine and improve the TRAC program by gathering feedback from all participants, AQ customers, and the larger AQ team.

Questions about the TRAC Program? Please email: dcsa.quantico.dcsa-hq.mbx.aq-integration-office@mail.mil.

# NISPOM RULE IS HERE: GET PREPARED!

For generations of facility security officers (FSO), the National Industrial Security Program (NISP) Operating Manual, or NISPOM, has been the standard document guiding industry implementation of NISP security protocols. Undoubtedly, many dogeared versions with heavily highlighted citations are sitting on FSO desks across the country.

All of that changed on December 21, 2020, when the Federal Register published the final rule titled "National Industrial Security Program Operating Manual (NISPOM)" (32 CFR part 117). No longer was the NISPOM a "manual" per se, it was now codified in statute as the "NISPOM Rule".

The Rule went into effect on February 24, 2021, with a six month implementation period for industry. The new NISPOM Rule is intended to better align with national policy for the protection of classified national security information disclosed to or developed by contractors, licensees, grantees, or certificate holders to prevent unauthorized disclosure, address changes in laws/regulations, and enhance the protection of classified material that contractors access or possess.

It prescribes industrial security procedures and practices under Executive Order 12829, sets requirements, restrictions, and other safeguards to prevent unauthorized disclosure and protect special classes of classified information, and aligns with 32 CFR part 2001, in a manner equivalent to the protection of classified information within the executive branch of the U.S. government.

While the Rule largely mirrored the legacy NISPOM, there were several significant changes, in addition to the format

- The Rule incorporates the requirements of Security Executive Agent Directive (SEAD) 3, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position." SEAD 3 requires reporting by all contractor cleared personnel who have been granted eligibility for access to classified information.
- The Rule provides for a single, nationwide implementation plan, which will include SEAD 3 reporting on specific activities that may adversely impact cleared contractor personnel's continued national security eligibility, such as foreign travel and foreign contacts.
- The Rule also implements the provisions of Section 842 of Public Law 115–232, which removes the requirement for covered National Technology and Industrial Base (NTIB) entities operating under a special security agreement (SSA) to obtain a National Interest Determination (NID) as a condition for access to proscribed information.

In response to the shift from manual to rule, DCSA created and published resources to assist cleared industry in better understanding what is required for compliance. More than 5,000 users have visited the NISPOM Rule webpage, close to 2,000 people have watched the "Ready for the Rule" video, and more than 3,000 users have used the NISPOM Cross Reference Tool — a deskside aid linking the familiar NISPOM table of contents with the corresponding section of the new NISPOM Rule.

## HOW TO PREPARE

To comply with the NISPOM Rule, cleared industry should plan to implement changes by September 2021. An industry security letter (ISL) will be coming out to provide guidance on the exact date and when previous NISPOM policy (DOD 5220.22-M) will be cancelled. Until then, DOD 5220.22-M will remain in effect.

**Step 1: CDSE Cross Reference Tool**. Download the 32 CFR Part 117 Cross Reference Tool from the DCSA website. It maps sections familiar to you in the NISPOM Manual to the new NISPOM rule.

**Step 2: Key Changes**. Familiarize yourself with the NISPOM rule's language, requirements, and key changes.

**Step 3: Industrial Security Letters**. Look for additional clarification and guidance in upcoming ISLs addressing topics such as 32 CFR Part 117 Implementation, SEAD 3 Reporting Requirements, and Top Secret Accountability, among others.

**Step 4: Implementation**. Take deliberate action during the implementation period to update and enhance your practices and procedures as necessary. Ensure that those affected in your organization are aware of what will be expected of them under 32 CFR Part 117.

## DCSA IS HERE TO HELP!

For additional resources, please visit:
https://www.dcsa.mil/mc/ctp/NISPOM-Rule/

## NISPOM HISTORY

| | |
|---|---|
| 1993 | In June 1993, the Defense Investigative Service (DIS), a DCSA predecessor, was directed to assume responsibility for finalizing the draft NISPOM. The team completed their draft NISPOM in October 1993. DIS began implementation of many of its provisions immediately. |
| 1995 | The NISPOM was first published in April 1995 as DoD Manual 5220.22. The NISPOM replaced the nearly 45-year old Defense Industrial Security Program and its Industrial Security Manual. |
| 2006 | Subsequent updates to the NISPOM included a major reissuance in February 2006. |
| 2013 | DOD released Conforming Change 1 in March 2013. |
| 2016 | NISPOM Change 2 implemented in May 2016. |
| 2021 | NISPOM Rule went into effect on February 24, 2021. |

## KEY CHANGES INCLUDE:

- Section 117.7(b)(2): Senior Management Official (SMO)
- Section 117.8(a): Reporting Requirements
- Section 117.9(m); Limited Entity Eligibility Determination (Non-FOCI) and Limited Entity Eligibility
- Section 117.11(d)(2)(iii)(A); National Interest Determination (NID)
- Section 117.13(d)(5): Classified Information Retention
- Section 117.15: Safeguarding
- Section 117.15(d)(4): Intrusion Detection System (IDS) Installation
- Section 117.15(e)(2): Top Secret Information Accountability

**DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY**

27130 Telegraph Road
Quantico, Virginia, 22134

DCSA.pa@mail.mil

571-305-6562

www.DCSA.mil