Official Magazine of the
Defense Counterintelligence and Security Agency

Gatekeeper

Volume 3, Issue 2

DCSA IMPROVING SECURITY CLEARANCE PROCESS;

RESULTING IN IMPROVED TIMELINESS, QUALITY, LOWER COSTS

IN THIS ISSUE

ASK THE LEADERSHIP
DR. MARK LIVINGSTON

EXCELLENCE IN
COUNTERINTELLIGENCE

BOYERS POST OFFICE PROCESSES
OVER 6M PIECES PER YEAR

IN THIS ISSUE

FROM THE DIRECTOR 3

ASK THE LEADERSHIP 4

DCSA CONTINUOUS VETTING IDENTIFIES SECURITY RELEVANT ISSUES EARLY ENOUGH TO MITIGATE INSIDER THREAT CONCERNS.....7

SYSTEM LIAISON BRANCH SUPPORTS TESTING EFFORTS DURING NBIS DEVELOPMENT, GETS 'SNEAKPEEK' HANDS-ON ACCESS 9

DCSA SMALL BUSINESS OFFICE SUPPORTS DOD SMALL BUSINESS STRATEGY EFFORTS 10

SENIOR LEADERS PRIORITIZE MISSION, COMMITMENT TO WORKFORCE AND NATION AT OFFSITE 12

ELEVATING OUR NATIONAL SECURITY MISSION THROUGH A TRANSFORMED POLICY PROGRAM 14

DCSA ANNOUNCES WINNERS EXCELLENCE IN COUNTERINTELLIGENCE AWARDS 15

DCSA SERVES AS NATO SUB-REGISTRY FOR CLEARED INDUSTRY.....17

DATA VISUALIZATION DRIVES NEW WAYS TO ANALYZE AND INTERPRET DATA 18

EXTENSIVE COLLABORATION CRUCIAL TO CREATING ALLIANCE TO COMBAT THREATS 20

AGENCY LAUNCHES REDESIGNED WEBSITE 21

VISIT BY THE HONORABLE JOSEPH KERNAN 21

FBI DIRECTOR RECOGNIZES DCSA SENIOR INDUSTRIAL SECURITY REPRESENTATIVE FOR 'EXCEPTIONAL SERVICE'.....22

DCSA 'ABILITYONE' CONTRACTORS WORK AS FAMILY TO IMPACT NATIONAL SECURITY 24

DCSA BOYERS MAILROOM FEATURES UNIQUE ZIP CODE, HISTORY AND STORIES OF SERVICE 29

OKLAHOMA CITY BOMBING – WE REMEMBER 31

Vol 3 | ISSUE 2

DCSA Gatekeeper

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

FROM THE DIRECTOR

Many are tracking the multiple diverse, yet related, missions that came together to form DCSA. Comprehending the size and complexity of the consolidation of government security functions that led to our establishment can be daunting. Indeed, with more than 150 field offices and a dozen headquarters buildings in the National Capital Region alone, DCSA has resources and capabilities of which many are unaware. This Gatekeeper issue made me aware of one such hidden gem: DCSA has its own ZIP code.

As you will learn in this issue, the DCSA mailroom at Boyers, Pa. processes roughly 6 million pieces of mail per year—vouchers and inquiries from law enforcement, universities, and employers across the nation that are necessary to complete DCSA's background investigations. I have visited the personnel responsible for this effort and found a dedicated, motivated AbilityOne contract team executing operations with an efficiency that would put other post offices to shame. This team exemplifies the Gatekeeper culture of unwavering commitment to DCSA's mission, vision, and values, and I am pleased to see their story shared.

Another example of our Gatekeeper culture is found in our new Assistant Director for Personnel Security, Dr. Mark Livingston. Responsible for the largest and most widely known mission at DCSA—encompassing background investigations, adjudications, and continuous vetting—Dr. Livingston brings to the Agency extensive experience in intelligence and security. He is responsible for one of the biggest and most successful transformation and modernization efforts in the U.S. Government today, and the article about him demonstrates why we are confident that the effort will continue to exceed expectations.

The topics covered in this issue showcase the breadth and scope of DCSA's mission, extending from initiatives led by our Office of Small Business Programs to the Agency's industrial security support to NATO. It is an exciting time to be at DCSA, and I am proud to highlight these efforts. Although I am unable to comment on every article in this issue, I draw your attention to the closing page, where we reflect on those who lost their lives during the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995. That vicious attack took the lives of five Agency employees who reflected the same dedication and commitment to our nation's security as I consistently observe in our workforce today. They gave their lives as Gatekeepers before we were even using the term. As we pause to remember these employees and their service to our country, I thank you for yours.

Thank you for your partnership and continued support to DCSA.

William K. Lietzau
Director,
Defense Counterintelligence
and Security Agency

ASK THE LEADERSHIP

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

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

Dr. Mark A. Livingston was named the Assistant Director for Personnel Security, of the Defense Counterintelligence and Security Agency (DCSA), effective July 3, 2022. In this capacity, he oversees the sustainment, transformation, and integration of DoD Personnel Security and Suitability and Credentialing program within DCSA, dedicated to ensuring a trusted workforce for both the Department and the rest of the federal government.

Prior to joining DCSA, Livingston served concurrently as the Deputy Under Secretary of the Navy, Intelligence Security & Insider Threat and the Assistant Deputy Chief of Naval Operations for Manpower, Personnel, Training, and Education. In these roles, he led the Department of the Navy's National Security Enterprise.

He has over 41 years of government service including 21 years as a United States Marine. He is a combat veteran and served in Iraq.

In 2017, he served as the Senior Director of Security & Intelligence, Deputy Under Secretary of the Navy (Policy), where he was responsible for developing and issuing effective security & intelligence, and insider threat policy. He served as the principal advisor to the Deputy Under Secretary (Policy), Under Secretary of the Navy and Secretary of the Navy on all matters relating to personnel background investigations and personnel security for both the U.S. Navy and U.S. Marine Corps.

Livingston's past work also includes Federal Law Enforcement service as a Supervisory Special Agent, Pentagon Force Protection Agency, Senior Nuclear Reactor Specialist at the U.S. Nuclear Regulatory Commission, and Director of Corporate Intelligence Programs, Northrop Grumman Corporation.

He is a graduate of University of Maryland, University College, where he earned a Bachelor of Science in Psychology, a Master's in Human Resource Management, a Master's in Business Administration, and a Doctorate in Management.

QUESTIONS AND ANSWERS

We have your bio, but what would you like readers to know about you?

I think, the fact that from a personal perspective, I consider myself very lucky to be in this job. I think there is often the perception that for people who rise to the senior positions that it's been an easy path. For me, it's been a journey. I am proud of the fact that I started at the bottom and worked my way up in both my military and civilian careers. I think what may not be conveyed in my bio is my sense of duty and my work ethic. I work hard to be a servant leader who is very appreciative of this opportunity. I hope to live up to the expectations of all of the men and women of Personnel Security.

What brought you to DCSA and this job?

I have been in the intelligence and security field for 42 years and it's clear to me that the future of security is DCSA. I enjoyed great success in my other assignments and jobs but asked to be here. I think DCSA is a challenge that I am looking for and to have an impact. When you think about personnel vetting and how we conduct background investigations, that system was built over a half a century ago. We are breaking new ground at DCSA with new processes and new ways of doing things. We've seen more changes in the security field in the last five years than in the previous 50. And I think we'll see more changes in the next five than we've just seen. At DCSA, we are pioneers. We are improving processes, timeliness, outcomes and we're creating new solutions. It's a lot of work but it's exciting and I am so impressed with the people of DCSA.

Your portfolio includes all aspects of personnel vetting (investigation, adjudication, continuous vetting); functions that used to be separate. What is the value in bringing them under one umbrella?

I think first and foremost is synergy and effectiveness of the challenging and complicated processes of conducting background investigations, adjudications and vetting. Prior to my arrival, each of these organizations were hugely successful on their own, but I think together they are even stronger. And by synergy, I mean the overall process improvement efforts. By working together, we are more proficient and we have the opportunity to be even better. I am excited about the future of DCSA Personnel Security.

Implementation of Trusted Workforce 2.0, the new federal vetting model, is a high priority for DCSA. How is implementation going? What challenges do you see and what successes has DCSA realized?

In terms of implementation, I think we are on track. We're faster, more efficient, and our cost model is better due to our current process improvement. I think a lot of people think of TW 2.0 as the future and it is, but it's also happening right now. We are in the process of building a more secure future. From a national security standpoint, we are more efficient, at a lower cost and faster than ever before!

Anything new is always a challenge. Our biggest challenge is getting buy-in from stakeholders or other agencies. We successfully implemented TW 1.5 and we will do so with 2.0. The overall process, from investigation to adjudications and vetting is better for national security. We brought reciprocity timelines down from almost 100 days to five or less. And, we have a continuous vetting program that is ongoing, 24/7 identifying potential threats and problems in near real time, vice every five years. All of these successes, clearly benefit national security.

The National Background Investigation Services (NBIS) will be the IT system to fully implement TW 2.0. How is Personnel Security working with the NBIS team to ensure the system can support the personnel security mission?

Shortly after I arrived last summer, the Director informed me that delivering NBIS was his number one priority. So, it became my number one priority as well. I focused my entire team on not only continuing their current jobs, but also looking at how we could help ensure we were contributing to the successful delivery of NBIS. I have a senior leader dedicated to supporting NBIS and we have a number of people from across personnel security who are working NBIS issues every day to help build momentum for NBIS delivery. We believe in NBIS and are fully committed to its success.

As the federal government moves to TW 2.0, how do you see the role of investigator/adjudicator changing? What message do you have for the Personnel Security workforce?

There will always be a need for trained, professional investigators and adjudicators. Those are skillsets that have to be performed by humans. They cannot be performed by artificial intelligence or automation alone. Now that said, we can be more efficient and more effective in how we do those jobs, but they will not be replaced. The vetting space, if you will, is only going to grow and the status quo will not work anymore. We have to evolve and be ready to embrace a new way of doing our jobs. Technology will be vital to our collective future success.

Any final thoughts?

I would only add that when we think of national security, we think of personnel security and its three components. DCSA exists to deliver personnel and industrial security in support of national security. You simply can't have national security without DCSA and what we do.

Lastly, the men and women of DCSA/PS are impressive in every regard. I am so impressed with the work ethic, can-do spirit and selfless sacrifices to our work here. When you think of Personnel Security please think of them, because they are the real reason we are successful. I am grateful for the opportunity to lead Personnel Security. Our Personnel Security motto is, "People first—Mission always". Every day DCSA Personnel Security comes to work, we make national security better!

DCSA CONTINUOUS VETTING IDENTIFIES SECURITY RELEVANT ISSUES EARLY ENOUGH TO MITIGATE INSIDER THREAT CONCERNS

By Beth Alber
Office of Communications and Congressional Affairs

In conjunction with Trusted Workforce 2.0 (TW 2.0), the Defense Counterintelligence and Security Agency is implementing Continuous Vetting (CV) to mitigate vulnerabilities in real time. Under the CV process, trusted individuals undergo continuous review to ensure the government and public's confidence that the individual will continue to protect people, property, information, and mission. The program is supported by automated record checks that pull data from data categories such as financial activity, criminal behavior and terrorism databases.

The goal of CV is to identify security relevant issues in near 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, to ensure classified information remains protected while conducting the appropriate investigation to collect the facts and make the appropriate adjudication of the issue.

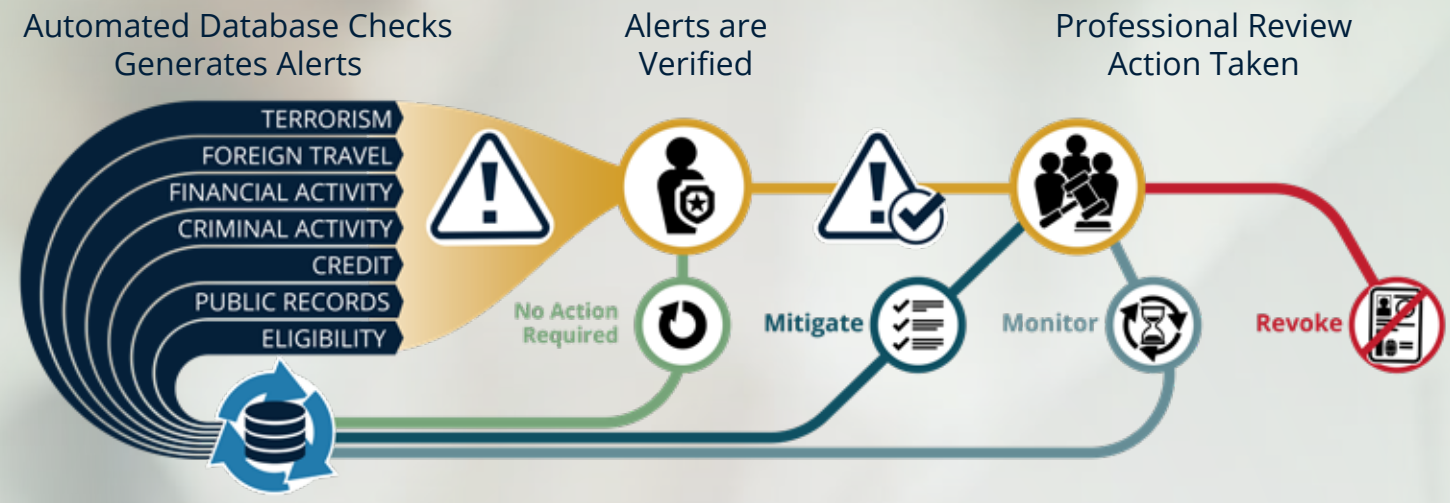
When DCSA receives an alert through CV, it assesses whether the alert is valid and meets certain threshold criteria for further investigation. DCSA investigators and adjudicators then gather facts and make clearance determinations. CV helps DCSA mitigate personnel security situations before they become larger problems, either by working with the cleared individual to mitigate potential issues, or in some cases suspending or revoking clearances. Under the periodic reinvestigation (PR) model, unreported issues would most likely be identified every five years in the case of Top Secret clearances and 10 years for Secret. For individuals enrolled in CV, the average to identify an issue for an individual with a Top Secret clearance is two years, seven months, and seven years, one month for a Secret clearance.

The majority of alerts received by DCSA are for financial considerations or personal conduct. For example, DCSA received an alert on an individual with a Secret clearance that was adjudicated in May 2019. In December 2021, VRO sent a Request for Action with a Continuous Vetting Action Report to the subject's Security Management Office to notify them that the individual had accumulated more than $57,000 in delinquent debt and had recently filed a Chapter 13 bankruptcy. The DCSA Consolidated Adjudication Services reviewed the material, determined the situation was isolated, the individual was taking positive action to address the debt, and followed up with a favorable eligibility determination. CV led to early detection of delinquent financial information seven years, six months before the next PR under the legacy model.

Another example occurred in January 2023, when DCSA received a critical alert for an individual with a Secret clearance that was adjudicated in July 2020. The alert indicated that the individual was charged with attempted murder. Vetting Risk Operations (VRO) validated the alert, developed information and notified relevant law enforcement, insider threat hubs, and the individual's chain of command. This information was developed and released within days of the attempted murder charge, and seven years, six months before the next PR under the legacy periodic reinvestigation model.

In addition to DOD affiliates, DCSA supports numerous federal partners by providing CV as a service. As an example, on December 28, 2022, VRO received an alert for an unreported in-state warrant for battery and criminal mischief-damage. By the next business day, VRO sent a Continuous Vetting Action Report to the federal customer for notification and determination of further action. As the individual had just been cleared with a Secret investigation

THE CV PROCESS



in January 2022, the use of CV led to early detection of this criminal activity nine years, 28 days, before the next PR under the legacy model.

The Director of National Intelligence, as the Security Executive Agent, sets policy for CV standards and defines what data sources must be used to in making adjudicative decisions under CV. A fully compliant CV model must include data sources within the seven mandated continuous vetting categories such as: Terrorism, Criminal Activity, Foreign Travel, Financial Activity, Credit Checks and Public Records. Accessing, ingesting, verifying and applying the volumes of CV data required for a cleared DoD population of 3.7 million personnel is a daunting job.

As a result, DCSA worked with the Executive Agents and Performance Accountability Council Program Management Office to establish policy allowing DCSA to incrementally approach TW 2.0 by implementing CV in two transitional phases —TW 1.25 and TW 1.5. Implementing CV using this phased approach enables DCSA to enroll populations in high-value continuous vetting checks as it works through automation to more efficiently address the full TW 2.0 data source requirements. Ultimately, the role of CV in the TW 2.0 framework is to enhance security, allow for greater reciprocity between organizations, and generate efficiency across the personnel vetting enterprise.

SYSTEM LIAISON BRANCH SUPPORTS TESTING EFFORTS DURING NBIS DEVELOPMENT, GETS 'SNEAKPEEK' HANDS-ON ACCESS

By Amanda Graham
Background Investigations

If there is one constant in the world of Personnel Vetting, it is change. The National Background Investigation Services, or NBIS, is the newest change to the background investigation landscape. When finished, NBIS will be the federal government's one-stop-shop IT system for end-to-end personnel vetting — from initiation and application to background investigation, adjudication, and continuous vetting.

Throughout the development of NBIS, the System Liaison branch within Personnel Security/Background Investigations' Customer and Stakeholder Engagements directorate, has partnered with the DCSA Program Executive Office (PEO) for NBIS testing efforts. Beginning with the first code releases, System Liaison has provided subject matter experts to the NBIS testing. This ensures the functionality that is necessary for customers to conduct their personnel vetting processes are available and working as expected, prior to being put into production. This testing has also given the System Liaison branch the opportunity to get early, 'sneakpeek' hands-on access to the new system prior to it being fielded. This experience is critical for System Liaison to be able to assist customers once they begin using, and require support in, NBIS.

System Liaison will continue to support the existing personnel security systems (Electronic Questionnaires for Investigations Processing (e-Qip), Defense Information System for Security (DISS), Fingerprint Transaction Systems (FTS), Central Verification System (CVS), and Personnel Investigations Processing System (PIPS)) until they have been sunset. No matter which system a customer agency is working in, System Liaison is ready to support.

One area of support that has never been offered in the past is applicant or subject support. The Customer Engagements Team within System Liaison is tasked with assisting applicants with accessing eApp, the portion of NBIS that applicants use to complete their standard forms for background investigations. In the past, the customer agency was responsible for supporting their own applicants. To ensure consistent and readily available support, DCSA made the decision to make this a service performed by dedicated customer service professionals assisting subjects with system access and answering any and all questions regarding the completion of the standard form for their background investigation. Whether an agency user, or the subject of an investigation, System Liaison is the one-stop-shop for NBIS support. For all of Customer and Stakeholder Engagements, and specifically System Liaison, customer service is at the core of their mission. On a daily basis, leadership in this mission space looks at key performance indicators (KPIs) and data to drive decisions on how best to provide support. Hold times for customer contacts are routinely measured in seconds, and a live customer service professional, who has subject matter expertise, is available to assist. DCSA recognizes that change is difficult, and therefore wants to provide the resources necessary to make this transition as seamless as possible.

Part of the Scaled Agile Framework of software development which NBIS is utilizing, is the idea of constant improvement. The tier one assets at System Liaison that are interacting with customers will record the reason that agencies reached out for support, and partner with the PEO to provide solutions to improve the user experience. The System Liaison branch prides itself on being the voice of its background investigation customers, and as such, will continue to represent the needs of the customers in all software development activities. By providing direct support to customers, or indirect support in development activities, System Liaison is 100 percent dedicated to the success of its customers, and the NBIS program.

DCSA SMALL BUSINESS OFFICE SUPPORTS DOD SMALL BUSINESS STRATEGY EFFORTS

By Beth Alber
Office of Communications and Congressional Affairs

"Small businesses are the engines of our economic progress; they're the glue and the heart and soul of our communities," said President Joseph Biden during a White House press briefing in February 2021.

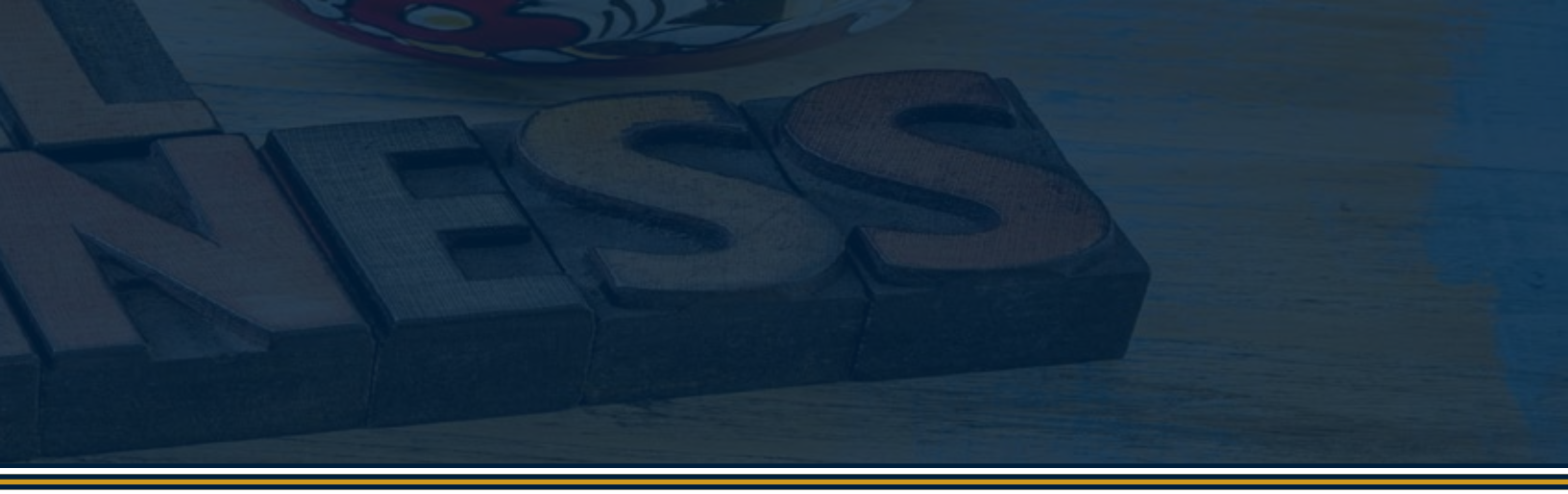
In the Department of Defense, "Small business participation in defense procurements as prime and subcontractors is vital to the defense mission, competition, and the health of the Defense Industrial Base (DIB)," as stated in the February 2022 DOD Report—Status of Competition within the Defense Industrial Base from the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD/A&S).

Yet, over the past decade, small businesses in the DIB shrunk by over 40%, as noted in the DOD Report. According to Deputy Secretary of Defense Kathleen Hicks, the data shows that if the DIB continues along the same trend, DOD could lose an additional 15,000 suppliers over the next 10 years.

In an effort to counter that trend, the National Defense Authorization Act for FY 2021 directed the Secretary of Defense to update the DOD Small Business Strategy, focusing on three objectives-- Improve management practices, ensure small business activities within the Department better support National Security priorities, and lastly, strengthen the Department's ability to engage and support Small Businesses.

Within the third objective, the Defense Counterintelligence and Security Agency was charged with conducting training to help educate small businesses on the risks of Foreign Ownership, Control, or Influence (FOCI).

Foreign investment plays an important role in the U.S. Industrial Base; however, DCSA ensures that no foreign business entities are able to affect the management or operations of any company in a manner that may result in unauthorized access to classified information or may adversely affect the performance of classified contracts. DCSA reviews a company's FOCI factors as part of the facility clearance process and throughout the life of the facility security clearance.



In support of the DOD Small Business Strategy, the Office of Small Business Programs and Industry Engagements (OSBP) coordinated with DCSA Industrial Security Facility Clearance office, and the OUSD/A&S Small Business Office to set up training opportunities to educate small businesses on identifying threats and the corrective action plans to mitigate known FOCI risks.

For the past year, DCSA OSBP and the Facility Clearance Office have spoken at a variety of conferences and symposiums, as well as providing one-on-one training and outreach to the DOD Industrial Base in an effort to reduce the vulnerability of the DOD Small Business Supply Chain.

“The DOD Small Business Strategy discusses the importance of helping to protect the Small Business Industrial Base against targeting of our smallest and most innovative companies through controlled access to rare raw materials, supply chains, and through FOCI,” said Dr. Ruby Crenshaw-Lawrence, chief of the DCSA OSBP. “DCSA was specifically highlighted among its peers as having the mechanisms and mission in place to support this effort.”

As part of the DOD Small Business Strategy, the Department established a Small Business FOCI Working Group to explore additional steps to help educate small businesses on the various aspects of FOCI while ensuring the Department strikes the right balance between taking additional measures and minimizing regulatory burdens that may deter small businesses from wanting to do business with DOD.

“Helping to protect the DOD Small Business Industrial Base from the threats outlined in the DOD Small Business Strategy is critical to economic and national security,” said Dr. Lawrence. “DCSA OSBP is proud to be a part of this important effort.”

SENIOR LEADERS PRIORITIZE MISSION, COMMITMENT TO WORKFORCE AND NATION AT OFFSITE

By Daniel J. Lecce
DCSA Deputy Director

The Defense Counterintelligence and Security Agency (DCSA) is no longer a new agency, and is at an inflection point. The agency's first five-year Strategic Plan, focused on meeting challenges presented by an evolving and increasingly complex threat environment, is well underway. The workforce continues to show unwavering commitment to DCSA's mission, vision, and values. To ensure DCSA continues to effectively deliver its mission and maintain national security, leaders across the agency came together during a Senior Leader Offsite this winter to discuss the current threat landscape, hold collaborative discussions on Strategic Plan implementation and priorities, and define specific actions required to support an inclusive, unified Gatekeeper culture.

STRATEGIC PLAN IMPLEMENTATION PROGRESS

The current threat environment is more complex and volatile than ever before, as evidenced by rapidly changing advances in technology and challenges from our adversaries in nearly every domain. In response to these challenges, the DCSA FY2022-2027 Strategic Plan aligns with broader intelligence and defense strategies and lays the foundation to resource DCSA's expanding missions.

During this winter's offsite, senior leaders from every mission area and support office provided updates and invited discussion focused on the transformation projects they are leading. Highlights include:

- Personnel Security's top priority is National Background Investigation Services (NBIS) deployment and Trusted Workforce 2.0 implementation, with NBIS and mission experts working together to mature functionality and ensure successful adoption.
- Industrial Security strives to match the rising threat posed by China and other near-peer threats by bolstering National Industrial Security Program (NISP) coverage, focusing on the entire Defense Industrial Base, and deploying technology to support emergent threats against the classified and unclassified industrial base.
- Counterintelligence and Insider Threat is heavily focused on Defense Insider Threat Management and Analysis Center (DITMAC) modernization as well as expanding the Counterintelligence workforce and capabilities. These efforts will improve CI coverage for DCSA missions, the Defense Security Enterprise (DSE), the Intelligence Community, and NISP.
- Security Training is hard at work building a credentialing framework, modernizing training tools, and conceptualizing a DCSA Academy and National Security Training Center that delivers comprehensive training to DCSA, the DSE, and security professionals supporting the United States government.
- DCSA continues to integrate its nationally distributed field workforce with the maturation of the Field Operations and the establishment of regional directors.
- Background Investigations' inventory reached a nine-year low during the second quarter of Fiscal Year 2023 with a total of 153,000 cases, the lowest since March 2014.
- DCSA is hiring across the agency! The Human Capital Management Office has made great strides in its hiring surge, averaging about 80 hiring actions a month in FY23. This is double compared to previous years.
- DCSA enabling support functions continue to leverage and build out Enterprise Service Delivery, enabling a productive work environment through

mission-enhancing processes, policies, and automation.

- DCSA is establishing an Operations Center to ensure realtime operational situational awareness and to best manage risk to operations and the workforce. The goal is to develop a common operating picture to facilitate unity of command, clear consistent, and timely communications, and comprehensive security risk management.

Senior Leaders participate in Unity of Effort Workforce Action Plan facilitated discussion.

Following each presentation, senior leaders provided insights on how to advance the Agency's mission and inspiring diversity of thought and perspective. While DCSA has made tremendous strides since its inception, Strategic Plan implementation updates illuminated some focus areas that cannot wait, such as the need to learn internal processes to enable the workforce to operate efficiently. Each mission area and functional support element must work together accomplish today's mission, while continue to look forward to counter future threats.

UNITY OF EFFORT—BUILDING DCSA'S CULTURE

When DCSA was created in 2019, the agency combined numerous organizations into one. Each legacy organization brought their own distinct culture informed by proud histories supporting United States national security. Now, DCSA is building upon the strength of its legacy cultures to forge one cohesive Gatekeeper culture that brings together the best of our collective talents and our commitment to serve our nation. Establishing and maintaining a strong, common DCSA culture is paramount to defending the Gate—protecting our nation's most sensitive information.

Culture is a major component of the Unity of Effort goal in the DCSA Strategic Plan, focused on Agency's values of people, mission, service to nation, integrity and innovation. These are not just words, but a way of life. In pursuit of this goal, we embarked on a Unity of Effort Roadshow at the end of last year. The Roadshow and its accompanying Unity of Effort Culture Survey not only provided the opportunity for leadership and the workforce to engage, but also allowed the workforce to provide feedback on their experience at DCSA. Combining this feedback with that from the Federal Employee Viewpoint Survey allowed leadership to define actions the agency must take to nurture a strong and enduring DCSA culture embodied by a workforce that is equipped to effectively and efficiently serve on DCSA's mission. Focus areas included: employee retention; empowering supervisors; opportunities for professional growth; leadership investment, responsibility, and accountability; Agency communications; and integration across the Agency.

On the final day of the offsite, senior leaders came together to create the first iteration of an action plan that addresses key areas of improvement across the agency. This plan, and leadership's dedication to executing it, is crucial to developing a strong, unified DCSA culture—which is fundamental to our success. In continuing to strengthen unity of effort across the agency, DCSA is equipped to secure the nation against serious and evolving threats head-on.

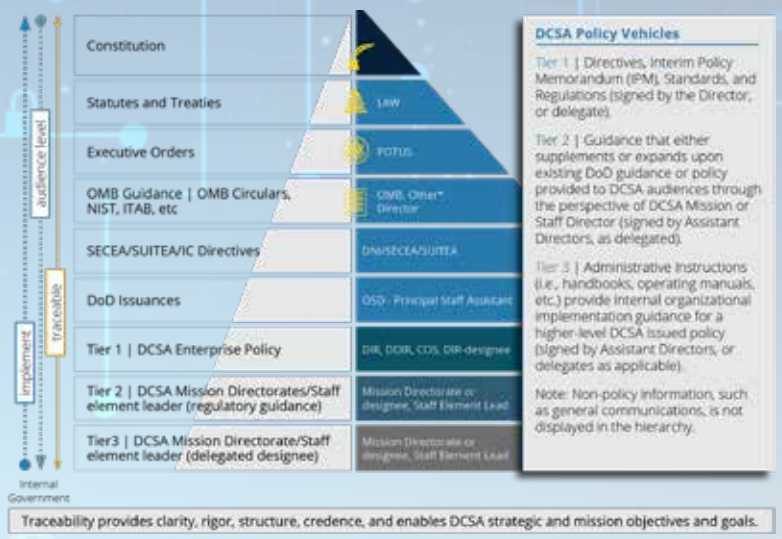
WHERE WE GO FROM HERE

DCSA is uniquely postured to accomplish its critical mission and enterprise goals to answer the ever evolving security challenges our nation faces. DCSA's commitment to its workforce and our nation is that we will have the right people, in the right place, at the right time to meet any security challenge our nation

ELEVATING OUR NATIONAL SECURITY MISSION THROUGH A TRANSFORMED POLICY PROGRAM

WHAT IS ALL THIS TALK ABOUT POLICY AND WHY IS IT IMPORTANT?

Policy is the bedrock of the nation. In fact, the national security work the agency does as Gatekeepers is required and implemented through various higher level governing policies developed under the rubric of the U.S. Constitution. As such, it is important that the agency create a formalized and structured policy program. To better align policy development and implementation with DCSA's strategic goals and track to DOD and national strategies, the DCSA has established an Enterprise Policy Program (EPP).



Traceability provides clarity, rigor, structure, credence, and enables DCSA strategic and mission objectives and goals.

Since forming DCSA in 2019, the agency's policy development and implementation efforts have followed a non-integrated path, with each DCSA element largely pursuing its own policy priorities with limited policy collaboration. While this siloed construct has enabled legacy agencies, and thereby new DCSA elements to maintain individual missions and operations, it produced a policy environment that does not scale to the demands of the agency's growth and strategic direction. Furthermore, it does not meet the workforce's expectation for consistency and clarity in policies/procedures. The complicated nature of today's world means that situations, threats, and trends rarely fall under the purview of only one mission. It requires greater integration and unity in policy formulation and the issuance process.

Creating a Best of Class Program

To design the EPP, DCSA leveraged best practices from long-standing successful policy programs across National Geospatial-Intelligence Agency (NGA), Defense Intelligence Agency (DIA), and Defense Contract Management Agency (DCMA).

The EPP transforms DCSA's policy making doctrine, applying reliable, consistent, and repeatable processes to promote integration, alignment, and transparency throughout the policy making and related procedural implementation processes.

The agency's policy program will be managed and overseen through a central policy office that relies on decentralized procedural implementation within each DCSA mission, staff, and program office. This model promotes more collaboration and integration to provide clarity, consistency, and improves the structure of DCSA policies and procedures.

Over the remainder of Fiscal Year 2023, the agency will conduct a top-down review of existing DCSA policy and procedures, which will set the stage for clear, consistent, and updated policies. Concurrently, those policies will be cataloged in an online library accessible to staff across the enterprise. Through these near term activities, continued stakeholder collaboration, and partnership from peer agencies, DCSA's EPP is employing a best-of-class policy program that improves traceability and scales to better posture DCSA to defend national security.

DCSA ANNOUNCES WINNERS OF EXCELLENCE IN COUNTERINTELLIGENCE AWARDS

Lockheed Martin Corporation, Old Dominion University, Orbit Logic, and Qorvo, earned the FY21 Defense Counterintelligence and Security Agency (DCSA) Excellence in Counterintelligence (CI) Award in August 2022.

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.

The following highlights each winner's FY 2021 efforts and how they achieved excellence in counterintelligence. For operational security reasons, specific details of operations and investigations cannot be provided.

The winners, in alphabetical order, are:

LOCKHEED MARTIN CORPORATION

Lockheed Martin Corporation (LMC), headquartered in Bethesda, Md., is a global security and aerospace company employing approximately 110,000 people at over 590 facilities in 50 states throughout the U.S. and in 52 nations and territories worldwide. The corporation is principally engaged in the research, design, development, manufacture, integration and sustainment of advanced technology systems, products and services. LMC is comprised of four business areas — LM Missiles and Fire Control, LM Aeronautics Company, LM Space Systems Company and LM Rotary and Mission Systems.

During an incredibly challenging environment of a world-wide pandemic in 2021, Lockheed Martin not only maintained a superior counterintelligence program, but continued to elevate their counterintelligence reporting, tools, and processes by aggressively seeking to identify threats and mitigate Foreign Intelligence Entity avenues of approach.

OLD DOMINION UNIVERSITY

Old Dominion University (referred to as Old Dominion), located in Norfolk, Va., is one of the largest universities in Virginia and was founded in 1930 by the College of William and Mary, the second oldest university in the United States. Originally established as an extension of William and Mary in Williamsburg, Va., and Virginia Polytechnic Institute in Blacksburg, Va., Old Dominion began as an institution primarily for teachers and engineers. The two-year school rapidly evolved into a four-year institution, and was granted independence in 1962 as Old Dominion College. It has an academic staff consisting of 3,000; a student base of over 19,000 undergraduates; and in excess of 5,000 postgraduates and PhD candidates. Additionally, 25% of Old Dominion students are military affiliated, with 769 international students from 89 countries. The university has been part of the National Industrial Security Program (NISP) since 2017. Old Dominion conducts some level of research and development in all technology spheres of the Industrial Base Technology List. Through routine working groups, Old Dominion has formed partnerships with at least three other academic members of the NISP, which has fostered the exchange of ideas, sharing of threat information, and group participation to protect collaborative research equities.

Throughout FY2021, Old Dominion conducted numerous onsite engagements with seven U.S. Government agencies while opening its doors to collaboration. This included CI, cyber, export control, and physical security spheres for a holistic approach to security.

ORBIT LOGIC INC.

Orbit Logic Inc. (OLI), headquartered in Greenbelt, Md., is an aerospace planning and scheduling company, employing about 40 people, specializing in mission planning, scheduling and space situational awareness software. OLI services are available to configure, customize and integrate OLI's mobile, web-based, desktop, and flight software applications.

OLI senior leadership and operational support staff, based on their own research and initiative, standing NISP directives and policies, and U.S. embargo regulations, developed extremely efficient and effective security protocols to control the purchase and distribution of their high resolution satellite imagery services. In addition to CI and Insider Threat training, OLI employees attend training in the identification of suspicious emails, operations security and Supply Chain Risk Management, presented by the supporting DCSA counterintelligence special agent in a virtual learning environment, due to COVID-19 restrictions. The company's cooperation allowed DCSA's collections and partnerships to truly maximize the technical capabilities of multiple agencies and enabled near-real time information to adjust intelligence Community (IC) activities. Moreover, the information OLI provided reached the highest levels of the U.S. government, including the President of the United States and key White House staff.

QORVO INC.

Qorvo Inc., headquartered in Greensboro, N.C., is a global semiconductor and electronic component manufacturing company employing over 8,000 people in over 45 facilities in the United States and around the world and is a Trusted Foundry under the NISP. Qorvo manufactures monolithic microwave integrated circuits used in most electronic equipment used by DOD.

Qorvo' s senior leadership, combined with extremely competent CI and security supervisory professionals, established highly impactful standards for supporting company efforts within the NISP directives and policies. The robust Insider Threat program at Qorvo-Texas, LLC is extremely effective in preventing loss of sensitive information. The company's CI experts aggressively delivered impactful and frequent CI awareness training that employees retained and applied to asset protection. Their suspicious contact reporting is exceptional in comparison to other defense contractors of similar complexity.

Qorvo is a significant partner in the IC. Qorvo participates in a robust and effective Cleared Contractor Counterintelligence Working Group (C3WG). While the pandemic produced restrictions precluding official C3WG events in 2021, their professional support to DCSA and CI components from other OGAs enabled the collection and subsequent production of numerous intelligence information reports that highlighted aggressive FIE activities.

AWARD NOMINATIONS

Candidates for this award are identified by DCSA field personnel and formally nominated by a panel consisting of the DCSA region 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.

DCSA SERVES AS NATO SUB-REGISTRY FOR CLEARED INDUSTRY

NATO Headquarters, Brussels. (NATO photo)

By Donna Newsom
International and Special Programs

The North Atlantic Treaty Organization (NATO), established in 1949, is a political and military alliance created to safeguard the freedom and security of its member countries. NATO members consult and cooperate in the fields of security and defense, and may create and possess information for strategic use by its member nations.

When member nations possess any NATO information they must safeguard it appropriately. To maintain control of NATO information, NATO established a central distribution point, or registry, for the receipt and distribution of NATO documents within each NATO member nation. In the United States, the Central United States Registry for NATO classified information is located in the Pentagon and oversees the administration of the U.S. Registry and establishes all U.S. Sub-Registries to execute the accountability and security management of NATO classified information. Thus, each NATO member nation is responsible for the establishment of a Central Registry within their member state to serve as the distribution point for NATO.

DCSA is the NATO Sub-Registry responsible for the establishment, inspection and disestablishment of NATO Control Points (NCP) within cleared industry. In accordance with DOD regulations, facilities performing on NATO contracts must be established as an NCP in order to safeguard NATO SECRET information and above. The NCP authorizes a facility to receive and distribute NATO classified to personnel in the facility which it serves.

Cleared defense contractors should notify their Industrial Security Representative and the DCSA Sub-Registry, dcsa.stanag@mail.mil, when they are bidding on or awarded a NATO contract. The DCSA Sub-Registry coordinates with NATO contracting authorities to verify facility security clearances, issue NATO Facility Security Clearance Certificates, and obtain security provisions of contracts involving U.S. cleared industry. Upon notification from the facility, the Sub-Registry will schedule a telephonic interview to review the contractual security requirements and determine the need for establishment as an NCP.

Cleared facilities currently performing on a NATO contract should contact the DCSA Sub-Registry to obtain a copy of the newest NATO Security Directives and Security Guide to NATO Control Points.

DATA VISUALIZATION DRIVES NEW WAYS TO ANALYZE AND INTERPRET DATA

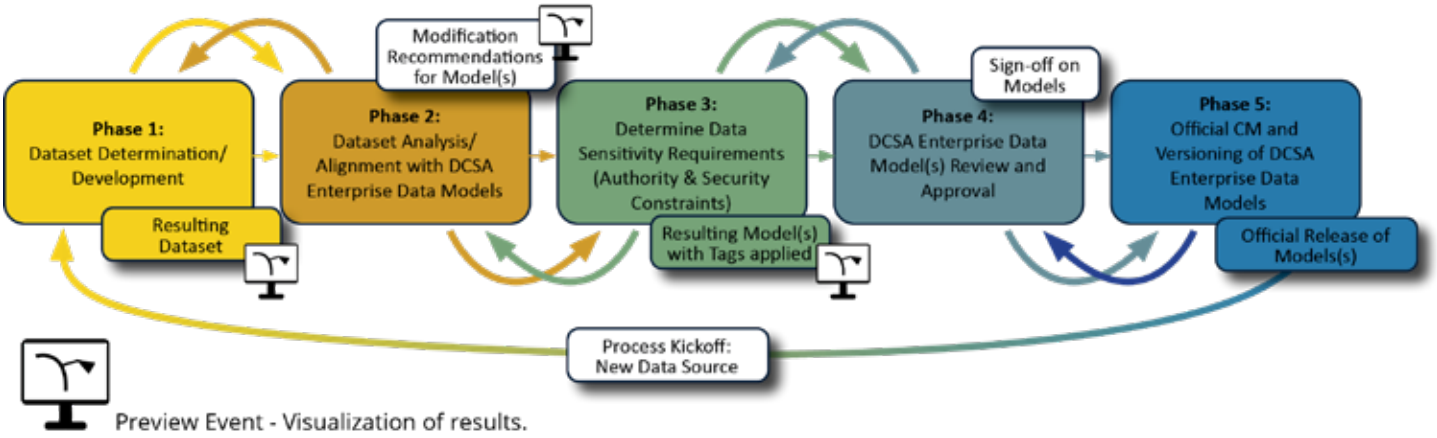


FIGURE 1: DCSA'S Data Transformation Process

By Ashley Dalisera and Diane Phan
Program Executive Office

As the old saying goes, a picture is worth a thousand words. This is what makes data visualization an important element of the analytic process and a key element in arriving at action-based findings from masses of data. More DOD organizations are using techniques to combine data from various sources, visualize it intuitively and discern trends or findings to make decisions. DCSA has taken the first steps in leveraging these techniques, specifically data visualization.

Data visualization is the representation of data through use of common graphics, such as node-link diagrams, charts, plots, infographics, and animations. These visual displays of information communicate complex data relationships and data-driven insights in a way that is easy to understand. Data visualization is an integral part of a larger data transformation process. Recently, the Program Executive Office (PEO) Artificial Intelligence (Ai) team developed a data transformation process as part of the Ai platform to support various mission partners. Data transformation is typically known as a process that is followed to convert data from one format or structure into another, and is regarded as a fundamental aspect of data integration and data management. Data transformation provides users with a unified view of data that originates from different sources.

The missions at DCSA use data that originates from different sources; stores data in different sources; in some cases, employs different data concepts; and represents data using different terminology, definitions and formats. Regardless of these differences, the common thread across all DCSA data is the need to understand and protect it. This is why DCSA's data transformation process takes into account the individual data elements and the information that results from these elements coming together.

As the process goes from one objective (or phase) to the next, a review event takes place where the results of the phase are visualized and presented to all team members (Figure 1). This visualization capability helps to ensure that all members of the team, regardless of position or specialty, can understand the results and provide feedback. Further, data visualization enables data identification and understanding of the relationships between the data concepts (how they work with each other) within and/or across missions. Feedback is incorporated into the data analysis results, and used to produce the final "blue-prints" which are then used for actual implementation of data systems and their operations.

DATA VISUALIZATION IN ACTION

The PEO demonstrated the data visualization capability with Industrial Security (IS) for a Foreign Ownership, Control or Influence (FOCI) use case. There are thousands of unreported, unidentified, and unmitigated critical vulnerabilities in the cleared industry population. Undetected and unmitigated risk is leading to compromise, loss, or damage of critical information and represents a grave threat to the Department's continued technological advantage over its adversaries.

Through this capability demonstration, the PEO team accomplished the following:

- Brought together IS data that previously could not be linked or visualized for analysis
- Validated tagging standards (Governance Metadata 0.2) and formalized Data Transformation Process
- Began to properly document National Industrial Security System (NISS) data elements to place under governance

In order to highlight the value of utilizing multiple data sources to improve the quality of information, the DCSA team worked to fuse a subsection of the NISS database with data provided by an external commercial source, a data aggregator providing corporate details about companies. The resulting information was displayed in a network graph to better allow users to explore the connections between companies, their sub-entities, and government agencies. This process included creating an alert to identify companies that had foreign addresses identified by NISS, but had reported no mitigation measures. Such alerts were displayed in a graph to inform analysts utilizing the tool of the potential risk.

The graph visualization capability leveraged to visualize NISS and the commercial data source is shown below (Figure 2). The tool set includes link analysis and entity exploration features. The visualization is expandable and modifiable to adjust the new information gathered from NISS and other sources with custom change alerts.

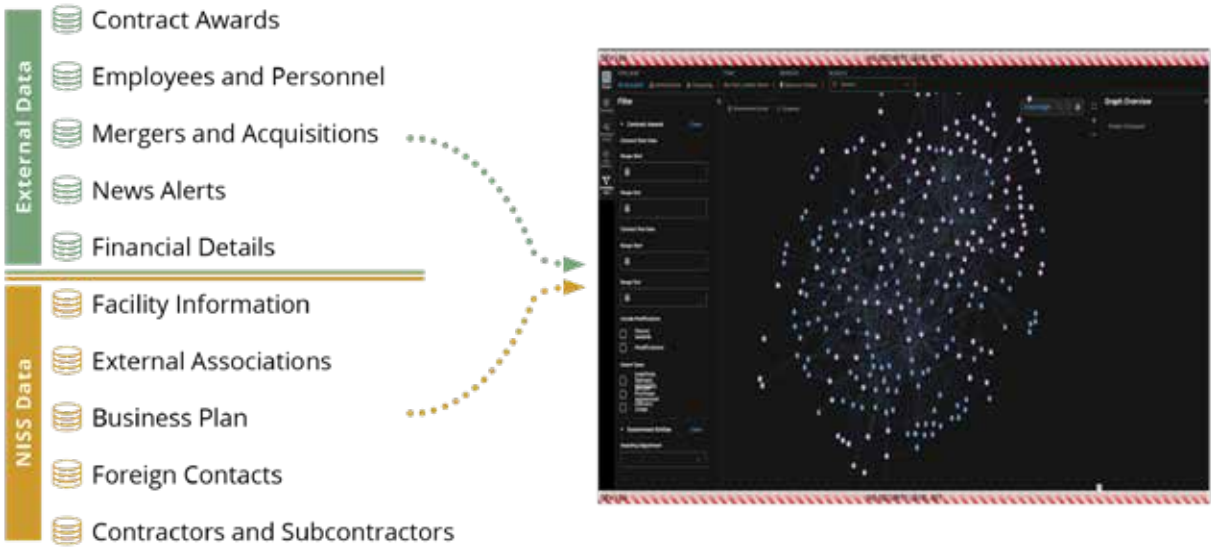


FIGURE 2

Through the use of data visualization, Industrial Security was able to link two high value data sets for the first time. This visualization effort enabled analysts to identify FOCI issues that had not been previously identified. By targeting variations illuminated through data visualization, the tool successfully supported IS analysts in mitigating risk. As the agency expands its use of data visualization and data transformation tools, they will assist in discerning trends or findings to make more informed decisions

EXTENSIVE COLLABORATION CRUCIAL TO CREATING ALLIANCE TO COMBAT THREATS

Alexandria 1 Field Office staff meet with CNA during a site assist visit. (Courtesy photo)

Companies and entities operating in the national defense sector encounter a myriad of persistent security challenges—from unauthorized access to national security information to the targeting of U.S. technologies. Faced with these sophisticated and diverse threats, security organizations are compelled to be vigilant, responsive, anticipatory and adaptable. Most important, they must be collaborative. Engagement with the Defense Counterintelligence and Security Agency, industry partners, government sponsors and other stakeholders is essential in creating a formidable alliance to combat the threats to national security.

The need for extensive collaboration and partnership is crucial, particularly in an operations environment that entails working shoulder-to-shoulder with warfighters and defense organizations in locations around the globe, on land and on sea. A good example is CNA, an independent, nonprofit research and analysis organization dedicated to the safety and security of the nation, which has been a critical participant in the national security domain for over 80 years. Within CNA is the Center for Naval Analyses, the only Federally Funded Research and Development Center (FFRDC) for the Department of the Navy that employs operations research to address military questions.

FFRDCs are research organizations dedicated to the mission success of a particular government department or agency sponsor. There are 42 FFRDCs, and the Center for Naval Analyses is the oldest organization among them. As an FFRDC, CNA has a unique relationship with its government sponsors, where understanding the value of a strong partnership is a critical component of its success. Appreciation of being a trusted partner extends throughout the organization. It has been invaluable in forging a collaborative relationship with DCSA and furthering its goal of building a highly effective compliance-based security program.

This collaboration is demonstrated by the CNA chief executive officer/senior management official's participation in quarterly meetings with DCSA regional headquarters. The CNA chief security officer routinely communicates and corresponds with the DCSA field office chief. In addition, the facility security officer and information systems security manager have regularly scheduled meetings/calls with their assigned industrial security representative and information systems security professional. These interactions provide opportunities to develop and validate solutions and strategies specific to business needs. CNA's approach is based on whole-company, compliance-first, risk-based, threat-driven and asset-focused principles tethered to a keen awareness of the ever-changing security landscape.

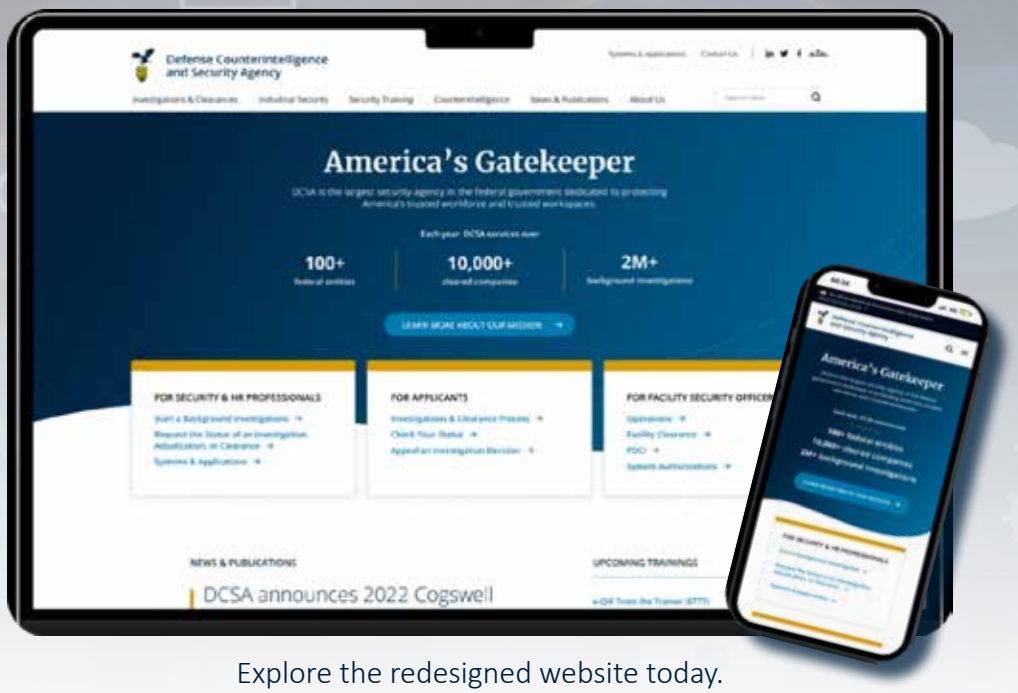
During the past two years, DCSA has conducted several site assist visits to CNA and participated in discussions on topics ranging from wireless headphones, fitness devices, and administrative inquiries to self-inspection checklists. These collaborations have prepared and positioned CNA to better leverage DCSA subject matter experts, and pool expertise and resources from other government organizations to counter current and emerging threats.

Instrumental in solidifying CNA's partnership with the Alexandria 1 Field Office were Ryan Franklin, field office chief; Nigah Ajaj and Kenneth Kisby, ISRs; Daniel Dorsey, team lead; and Moises Munoz, ISSP. Their responsiveness, genuine willingness to help, and level of involvement provided a framework for an enduring partnership, which is essential in safeguarding national security information and assets.

AGENCY LAUNCHES REDESIGNED WEBSITE

The Defense Counterintelligence and Security Agency (DCSA) launched a redesigned public website that is enhancing and enriching users' digital experience with increased functionality and navigation capability to DCSA content and services.

DCSA customers and stakeholders are encouraged to discover and navigate around the website where a more user friendly experience and easier access to information and services are available. Be aware that some URLs may change, so established bookmarks could result in error messages.



Explore the redesigned website today.

Visit by The Honorable Joseph Kernan

Defense Counterintelligence and Security Agency Director William K. Lietzau (left) hosted a tour of the agency headquarters and presented a DCSA award to The Honorable Joseph D. Kernan, former Under Secretary of Defense for Intelligence, at the Russell-Knox Building, Quantico, Va., recently.

(DOD photo by Christopher P. Gillis)

FBI DIRECTOR RECOGNIZES DCSA SENIOR INDUSTRIAL SECURITY REPRESENTATIVE FOR 'EXCEPTIONAL SERVICE'

By John Joyce
Office of Communications and Congressional Affairs

DCSA Senior Industrial Security Representative Mary Dean was looking forward to meeting FBI Director Christopher Wray while accepting a Letter of Appreciation on behalf of the Norfolk Citizens Academy Alumni Association (FBINORCAAA) on Feb. 15.

Dean—who works out of the DCSA Virginia Beach Field Office—was surprised to be sent a personal invitation to the event where Wray would address members of the press during a media availability at the FBI Norfolk Field Office.

Everything went according to plan with one exception. Wray personally presented the DCSA employee with an FBI letter of appreciation.

FBI Director Christopher Wray (center) presents certificates of appreciation to members of the FBI Norfolk Citizens Academy Alumni Association on Feb. 15. DCSA employee Mary Dean is second from left in the front row. (Photo courtesy of FBI)

"I was intending to be with others from our chapter to accept a certificate of appreciation for the chapter, but upon arrival, was pleasantly surprised with an individual certificate for exceptional service in the public interest," said Dean, who serves as the FBINORCAAA vice president. "I was happy to meet Director Wray personally and see that the director of the FBI is acknowledging the work that the chapter puts forth each year to serve the community and to aid the FBI in any way they need. I am but a very small part of an amazing group of people who serve the community. The director was very approachable and I enjoyed being able to meet and talk with him."

Wray also presented a certificate of recognition to the FBI Norfolk CAAA as a whole in front of the media.

"Strong partnerships are essential to the Bureau's mission, and building bridges between law enforcement and the communities we're sworn to serve and protect is crucial to fulfill that mission," said Wray. "We all have the same goal—to keep our communities safe. And the best way to do that is by working together."

The FBI Norfolk CAAA is a non-profit, volunteer organization that works in partnership with the FBI's Norfolk Field Office on community outreach programs promoting safety and security across the Hampton Roads region.

Moreover, Dean and her FBI Norfolk CAAA colleagues—representing diverse walks of life and professions from accountants and attorneys to social workers and hotel managers—are considered official ambassadors of the FBI to support its outreach efforts through education, events, and community service programs that improve public safety.

"Our members provide great resources to provide help and assistance to the FBI and the community," said Dean, regarding FBINORCAAA's staff of about 120 volunteers. "Over the past few years we have actually been even more outward facing than in the past. For example, in

the aftermath of the mass shooting at the Virginia Beach municipal center, we were very active in ensuring meals and supplies."

As the organization's vice president, Dean was part of the FBINORCAAA's efforts to assist the FBI and local law enforcement in the aftermath of the Walmart shooting in Chesapeake, Va., by providing meals and supplies as needed.

"We have an incident response team that works on responding to catastrophic events," said Dean. "Food and other supplies are needed and we make sure they get there and our coverage spans greater Hampton Roads all the way up to Eastern Shore."

Dean has been active in the organization's Law Enforcement Symposium since transferring to the Norfolk chapter in 2018. She is one of the leads in efforts to plan and host the symposium for local law enforcement to obtain the Virginia Department of Criminal Justice Services continuing education credits necessary to maintain their certifications.

"We do things as simple as helping with the massive Mayflower marathon food drive that hits both sides of the peninsula each fall. We supply manpower to help collect food and make boxes for families in need," said Dean. ""The FBI Norfolk CAAA educates in combatting and preventing human trafficking by giving presentations to the public. We also work alongside the FBI by adding extra hands in an annual event called Future Agents in Training for high school students considering a possible career with the FBI. The students are put through a program that is almost like a mini-academy, which includes running the students through the FBI physical test that they would have to pass when applying to be an agent."

The FBI Norfolk CAAA volunteers are graduates of the FBI Citizens Academy, an eight week program that gives business, religious, civic and community leaders an inside look at the FBI. Upon graduation, they provide the services and response to incidents that Dean cited as well as the following services to promote safety and security:

- Providing public education programs to raise awareness of community safety issues such as cybercrime, violent extremism, drugs, terrorism, gang activity, public corruption and other criminal activities.
- Equipping Hampton Roads citizens with information, tools and resources to address public safety issues such as opioid addiction, hate crimes, online scams, human trafficking, and active shooter situations.
- Hosting symposiums and events that facilitate collaborative relationships among federal, state, and local law enforcement agencies in Hampton Roads, and promote positive community and law enforcement relationships.
- Supporting FBI sponsored outreach and information programs to community citizens, businesses, religious organizations, government agencies, and other individuals and organizations vital to the Hampton Roads region.

"I do it for the same reason I'm an ISR (Industrial Security Representative) at DCSA—its for our nation and our communities and that's what we do," said Dean, a 2013 graduate from the Richmond FBI citizens Academy. "We conduct a lot of educational and training events for the public on how to protect themselves, protect our nation and protect their communities."

The FBI Norfolk Citizens Academy Alumni Association is part of the FBI National CAAA, an organization that joins together more than 42,000 community and business leaders who are dedicated to making our neighborhoods safer and serving as volunteers in 60 chapters around the nation, all comprised of those who graduated from a FBI's Citizens Academy program.

* The FBI Norfolk Citizens Academy Alumni Association is a nonprofit organization separate and apart from the FBI.

DCSA 'AbilityOne' Contractors Work as Family to Impact National Security

By John Joyce
Office of Communications and Congressional Affairs

Iron Mountain—where miners once dug deep for limestone—is now home to a team of contractors who dig deep within themselves while overcoming their disabilities to make an important impact on the Defense Counterintelligence and Security Agency (DCSA) Personnel Security Mission.

The Keystone Vocational Services contractors, who have disabilities ranging from blindness and low vision to being deaf or hard of hearing to learning and other disabilities, work underground surrounded by cavernous limestone walls at the mailroom in Boyers, Pennsylvania, via an AbilityOne contract to accomplish a vital mission.

The team - utilizing assistive technologies and creativity to innovate technologies and methods to get the job done - is accomplishing an important Federal Investigative Records Enterprise (FIRE) mission in support of national security.

In all, there are 40 Keystone employees with disabilities, mostly general and mail clerks as well as managers, collaborating with the government team at Boyers to fulfill contract requirements impacting FIRE—a component in the Background Investigations mission. FIRE is responsible for the processing, automation, and management of government-wide investigative records collection and analysis, and end-to-end case processing functions.

The Keystone AbilityOne team's mission—process approximately - 6.6 million pieces of mail annually while achieving mailroom goals and responsibilities. This includes processing incoming and outgoing vouchers and inquiries that are sent to and received from law enforcement, universities and employers across the nation in the course of DCSA background investigations.

Lacey Rasely conducts general clerk II technical functions using the Topaz Ultra, Acrobat Arm with Monitor, XY Table, and Zoom Text software.

The mailroom—officially known as the Document Processing Operations Center—is a beehive of activity as the contractors sort background investigation forms while securely processing thousands of documents via U.S. Postal Service, Federal Express, United Parcel Service, DHL and other carriers. They make it happen while using assistive technologies coupled with typical mailroom equipment such as envelope conveyers, mail scanners, folder inserters, label printers and the postage meter.

"It's a critical piece of our overall investigation process," said Mary Price, DCSA FIRE branch chief, regarding mail processed by the Keystone contractors. "When we have hardcopy mail such as fingerprints, our Keystone team manifests [lists the contents] that mail, so we can track it throughout the system. They also manifest outgoing material. So, if a package is inadvertently lost during shipment- we know exactly what's in that package."

"I'm helping with national security, but the job is helping me because it's full time meaningful employment that actually allowed me to get off of Social Security disability benefits," said David Miller, a Keystone employee working at the Boyers mailroom for more than five years as a general clerk. "This job enabled me to become more self-sufficient and earn my way in the world."

After a life changing event caused Miller to lose 100% of his eyesight without light perception, he spent 16 weeks training at a school for the blind, learning daily living skills, mobility with a cane, and adaptive software computer skills. At that point, he worked on an associate degree in applied science and business management, graduating summa cum laude.

When people in any organization approach their work as a family, the impact on their mission and personal lives is greater, according to Miller and his Keystone co-workers.

"There's no judgement here—it's all teamwork in a family atmosphere," said Tammy Currie, a mail clerk who commutes by van and bus in her three-hour round trip to Boyers because "I love my job."

Initially, the commute and work location in the Iron Mountain mine was a daunting experience for Currie who has severe claustrophobia and cried when she began her position two years ago. "I had a lot of disabilities throughout my life, but I like challenges," she recounted. "At first I was intimidated, but I considered it a challenge. I'm proud of myself and feel important doing what my job requires me to do for our country. Our national security is at stake and if I can do this, I can do anything."

What's more, Currie faced her fear of heights by joining several of her Boyers co-workers and her daughter, an Army National Guard soldier, on a skydiving expedition that began with a flight in a small plane. "All of our co-workers cheered us on," she recalled with a smile. "I try to be a good role model for my daughter and my co-workers. It's teamwork—we're always encouraging each other."

The Keystone team's encouragement includes checking with each other to see if a colleague needs advice, a helping hand or a head start and if so—rendering the assistance needed in any given situation.

"They're quite surprising around here. They will really surprise you when it comes to teamwork," said Keystone mail clerk Dale Harris while explaining how the Background Investigation outgoing vouchers and inquiries are processed and expedited at the mail room.

"At times, I've been ready to begin my next task after completing releases and would be taken by surprise," Harris said. "The labels for addresses are already typed in advance and packed; investigative materials are mailed out that day; or another task started. It's a great responsibility that we're dealing with, and this team spirit is essential to our success."

David Miller prints releases with JAWS software and the L3 system with a barcode reader at the Boyers mailroom.

Keystone general clerk Lacey Rasely, legally blind as a result of bilateral optic nerve hypoplasia, describes her cubicle as a spaceship with five computer screens, including three low vision monitors to enlarge the text and casework content.

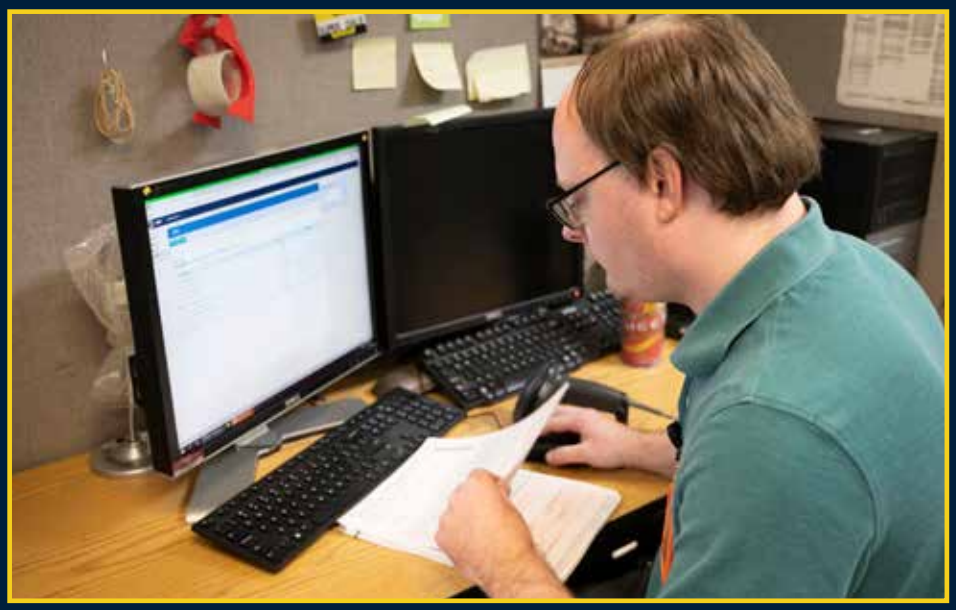
Rasely began working on the mailroom's folder team in 2017, recycling folders for copies of cases filed at Boyers. When the task became paperless, she transitioned to manifesting materials and is now engaged in auditing, quality control and special assignments.

"I'm honored that they let us do the things we do despite our disability," she said. "I really find satisfaction, especially when things come out well. I just love being a part of our contribution to national security while learning new things and helping DCSA accomplish what they need to do."

Keystone general clerk Heather Presnar—diagnosed with Stargardt disease, a juvenile macular degeneration when she was nine years old—did not let her vision stop her from playing sports or anything else in her life and career.

"It's nice that we have every type of equipment and resources imaginable so if I need a hand magnifier, there's one here. If I need a CCTV [closed-circuit television], there's one here," said Presnar. "So, every type of assistive technology is right at my fingertips, which is really nice. I don't think of myself as being really disabled, but it does help me perform the job. It makes a difference doing your work so you're not struggling trying to see different things."

Tammy Currie uses a light arch to process police department vouchers for outgoing mail at the Boyers mailroom.



Dale Harris prints releases at the Boyers mail room.

Prior to her current position with Keystone, Presnar worked in social services and the medical field. "It was definitely a huge change for me, but it's been a great opportunity," she said. "Everyone is out to help each other. I may be able to do one task for someone else who can't, so I'll help them, or vice versa. Our management is always willing to try new things to help us in any way. We are a great team and I mean everyone's there to put in that extra effort. There are also a lot of perks. The family atmosphere is like no other place. I like that—family."

The team's extra effort began in early 2017 when Keystone was awarded the AbilityOne contract. Since then Keystone managers and supervisors adapted former mail processing workflows to incorporate and support a process for employees with blindness, low

vision and other disabilities to assume the day-to-day workflows.

"It's the collaborative relationship with the government and utilization of our assistive technology that we bring to the table that truly empowers, engages and enables our individuals to be successful," said Brett Hedglin, Keystone program manager. "We have a tremendous amount of assistive technology at our disposal that we apply through grants and other means that some of our individuals rely on to do their job. Some of that is technological. Some of it is manipulative. We are applying different forms of assistance for our employees to utilize on the devices in government spaces as we work with the government team."

The assistance includes assistive technology solutions and innovations developed by Keystone supervisors and managers to enable their employees to successfully complete required tasks, projects and requirements.

Heather Presnar conducts case processing using an Acrobat Arm to scan mail with a UPS Trackpad handheld.

Greg Klamer loads business reply mail envelopes into the inserter for the voucher outgoing process.

"This contract with DCSA gives us all a sense of purpose and a reason to be proud of my government," said Keystone supervisor, Lonny Lemke, who examined the agency's mailroom processes to develop solutions that enable employees with disabilities to complete tasks independently. His innovations include safeguards on the envelope insertion machine; scanning boxes used to process government forms for attachments; templates for training on various government forms for manifesting purposes; and a light arch that allows people with limited vision to operate at a higher rate because of the reduced glare, shadows and adjustable brightness. Lemke also innovated jigs for mail packaging. A jig is a type of custom-made tool or template that allows for the control or motion of a process or another tool in order to enhance usability, safety, quality, accuracy and speed.

"The individual impact shines through everything in this contract from our employees to our leaders and collaborators on the government side," said Craig Felix, Keystone facility security officer and information technology manager. "The relationship that we have with the government team, our work and how we do it, as well as the location are important to each individual member of our team. The betterment of our employees is also very important to us and because of that, we are attracting individuals that are focused on the betterment of the processes.

The U.S. AbilityOne Commission is the independent Federal agency that oversees the AbilityOne Program, whose mission is to tap America's underutilized workforce of individuals who are blind or have significant disabilities to deliver high quality, mission-essential products and services to Federal agencies in quality employment opportunities.

The Commission administers the Program with the assistance of two central nonprofit agencies – National Industries for the Blind (NIB) and SourceAmerica—in accordance with the Javits-Wagner-O'Day Act. The U.S. AbilityOne Commission is the operating name for the agency, whose statutory name is the Committee for Purchase From People Who Are Blind or Severely Disabled.

AbilityOne Program

AbilityOne provides employment opportunities to approximately 40,000 people who are blind or have significant disabilities, including more than 2,500 veterans, the AbilityOne Program is among the nation's largest providers of jobs for people who are blind or have significant disabilities. The AbilityOne Program uses the purchasing power of the federal government to buy products and services from participating, community-based nonprofit agencies nationwide, dedicated to training and employing individuals who are blind or have significant disabilities. Through the AbilityOne Program, people who are blind or have significant disabilities enjoy full participation in their community and can market their AbilityOne-learned skills into other public and private sector jobs.

DCSA BOYERS MAILROOM FEATURES UNIQUE ZIP CODE, HISTORY AND STORIES OF SERVICE

A Civil Service Commission (CSC) experiment testing the ability of Iron Mountain-based employees to take on the workload of 10 National Agency Check with Inquiries (NACI) regional offices evolved over 46 years into a mailroom where millions of pieces of mail, including background investigation forms and documents are processed annually.

The experiment—a resounding success—began in 1977 when the CSC consolidated its regional NACI offices into one new center in Boyers, Pa. Initially, a massive volume of incoming and outgoing mail inundated the small Pennsylvania town's rural U.S. post office but a new zip code resolved the issue.

"The experiment was successful and on top of inquiries, we were also receiving requests for background investigations," said Lynn Craig, Defense Counterintelligence and Security Agency (DCSA) Privacy, Civil Liberties, and Freedom of Information (PCLF) Program specialist. "The U.S. Post Office quickly agreed to give us our own zip code so they would be less affected without hiring additional postal workers. Our mailroom also initiated a color envelope coding system to make it even easier for the postal service."

Craig—who experienced the mailroom's transformations since the experiment began—witnessed the NACI Center's transition from the CSC to the Office of Personnel Management (OPM) in 1979 and to DCSA in 2019 as it continued covering all correspondence transiting through the facility.

After 19 years as a government employee, Craig and her colleagues became federal government contractors performing the same NACI duties when OPM—in an effort to reduce the size of the civil service—privatized its federal investigative service.

"We didn't have a choice but none of the federal employees lost their jobs," recounted Craig, regarding the NACI transition to a United States Investigative Service (USIS) company in 1996. "One day we walked out of Iron Mountain as federal employees. The next day we walked in as contract employees doing the exact same work."

Nine years later, Craig left her position at USIS to take time off and attend college.

"The USIS contract was eventually broken up and awarded to other companies. Over time, specific sections of USIS transitioned back to government positions," said Craig who came back to the same position in 2010 as an OPM government employee.

"It's amazing to look back at how we first started when many people didn't think we'd succeed and look at us now," she reflected. "I'm very proud of all the innovations and proud of working here. I love it. The work is interesting. The people are top notch. We've got a really great environment to call our own here. We can do it and we've proved it throughout our transitions from government to the private sector and back to government while transferring among different agencies, and we're still here making a tremendous impact for national security."

We've got a really great environment to call our own here. We can do it and we've proved it throughout our transitions from government to the private sector and back to government while transferring among different agencies, and we're still here making a tremendous impact for national security."

~ Lynn Craig

As Craig looks back, she recalls the amazing stories that involve her government and contractor colleagues working to accomplish their mission to process and manage government-wide investigative records collection, analysis and end-to-end case processing functions.

"I have all kinds of stories but the information—the things that we do—touches all of our country. We deal with subjects here," said Craig, reminiscing about one particular subject. "He was a Marine and needed a copy of his Standard Form 86, Questionnaire for National Security Positions, for his next position designated as national security sensitive."

Craig recalled it was about 2 p.m. when he called, and that she explained the first-in and first-out process to expedite forms and documents. The Marine would have to stand by while the forms submitted ahead of him were processed.

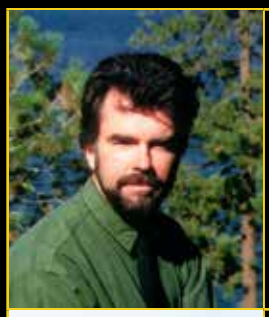
"He said, well ma'am, I'm supposed to have this at 8 o'clock this morning," recalled Craig, who responded by asking the Marine if somebody promised it would be expedited to the head of the line. "His answer was no, but he received an e-mail stating that the White House required a copy of his standard form right away. I said, 'Sir—can you hold on?' He said, 'yes.' I got the information and made him stay on the line. I transmitted it. That was probably 10 years ago, and to this day, when I see a Marine open up the door of the White House - that's my Marine. That's how doing this type of work makes you feel. He's going to be my Marine forever. I'm sure he's already gone but as far as I'm concerned, the Marine at the White House is my Marine."

OKLAHOMA CITY BOMBING – WE REMEMBER

On April 19, 1995, an ammonium nitrate fuel bomb, packed into a rented Ryder truck, exploded at 9:02 a.m. near the north side of Alfred P. Murrah Federal Building in downtown Oklahoma City, Oklahoma. The explosion killed 168 people, injured more than 650 others, demolished nine floors of the Murrah Building, and left a 30-foot-deep crater in the city square-block.

The Murrah building housed a mixture of government offices, including that of the Defense Investigative Service (DIS), the predecessor to the Defense Counterintelligence and Security Agency. The Oklahoma City Field Office was located on the third floor, just left of center of the building.

In April 1995, there were 12 employees assigned to that field office. Given the nature of their work, seven of the employees were not in the office — they were out running leads, conducting interviews, and one person was at the courthouse doing records checks. The five DIS employees killed in the explosion just happened to be in the office on that fateful morning. DCSA remembers.



Harley Cottingham

Peter DeMaster

Norma "Jean" Johnson

Larry Turner

Robert Westberry

Defense Counterintelligence and Security Agency

27130 Telegraph Road
Quantico, Virginia, 22134
DCSA.pa@mail.mil
571-305-6562
www.DCSA.mil