National Industrial Security Program Policy Advisory Committee (NISPPAC) Meeting
Wednesday, April 27, 2022 - 10:00 a.m. - 12:00 p.m.
National Archives and Records Administration (NARA)
Information Security Oversight Office (ISOO)
Meeting held virtually

Agenda

Welcome, Introductions, and Administrative Matters	**5 mins**
Action Item Follow Up	**5 mins**
Reports and Updates	
Industry Update	**10 mins**
Department of Defense (DoD) Update	**10 mins**
Defense Counterintelligence and Security Agency (DCSA) Update	**10 mins**
Office of the Director of National Intelligence (ODNI) Update Security Executive Agent	**5 mins**
Department of Homeland Security (DHS) Update	**10 mins**
Department of Energy (DOE) Update	**5 mins**
Nuclear Regulatory Commission (NRC) Update	**5 mins**
Central Intelligence Agency (CIA) Update	**5 mins**
Break	**5 mins**
Underwriters Laboratories (UL) Inc.	**10 mins**
General Services Administration (GSA) Safe Ordering Presentation	**10 mins**
Working Group Update	**10 mins**
Defense Office of Hearings and Appeals (DOHA) Update	**5 mins**
Controlled Unclassified Information (CUI) Update	**5 mins**
General Discussion, Remarks and Adjournment	**5 mins**

National Industrial Security Program Policy Advisory Committee (NISPPAC) Meeting Minutes April 27, 2022

I hereby certify that, to the best of my knowledge, the foregoing minutes are accurate and complete.

Heather Harris Pagán Signature

These minutes will be formally considered by the Council at its next meeting and any corrections or notations will be incorporated in the minutes of that meeting.

The NISPPAC held its 68th meeting on Wednesday, April 27, 2022, virtually. Mr. Mark Bradley, Director, Information Security Oversight Office (ISOO), served as Chair.

Dr. Jennifer Obernier, the primary NISPPAC member with the Navy, has departed and been replaced by Mr. Steve James. Additionally, the NSA alternate Shirley Brown has also departed. She's been replaced by Mr. Blane Vucci. The NASA primary, Kenneth Jones has departed as well. At this time, a replacement has not yet been designated. Mr. Bradley announced this would be Mr. Greg Pannoni last NISPPAC meeting due to retirement, who was the Designated Federal Officer for the NISPPAC.

Ms. Heather Sims, Industry Spokesperson, briefed that Industry created a newsletter to talk about who they are, and what they are trying to do. This was sent through the Cognizant Security Agencies (CSAs) to make sure that Industry is reaching those companies who are unaware they are represented at the national level for policy concerns.

She thanked the Memorandum of Understanding (MOU) members of the Industry NISPPAC for the working groups, collaboration, and for verifying that Industry gets the right people for the right skillset. She also thanked Mr. Matt Eanes, Director, Performance Accountability Council (PAC) Program Management Office (PMO), for ensuring that Industry had a voice when it comes to national-level personnel security reforms.

Industry has been reporting in on how Defense Counterintelligence Security Agency (DCSA) rolled out Department of Defense (DoD) oversight implementation for 32 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM). This was sent to DoD and to DCSA as a guideline on issues that Industry and DCSA can work on together as Industry is seeing variances in how certain parts of 32 CFR, Part 117 is being interpretation.

Industry is concerned about is the Defense Information System for Security (DISS) to the National Background Investigation System (NBIS) transition. Industry wants to ensure that they have an effective, trusted system in which they do not have to fix their own data.

Mr. Jeffrey Spinnanger, Director, Critical Technology Protection (CTP), Office of the Under Secretary of Defense for Intelligence & Security (OUSDI&S) thanked Mr. Pannoni for his time with the NISPPAC.

DoD introduced an amendment regarding reporting foreign travel associated with Security Agency Directive (SEAD) 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position.

The project that was sponsored at the Applied Research Laboratory for Intelligence and Security, (ARLIS), led to the development of a playbook aligned to Defense Information Systems Agency (DISA) and DCSA's current process guides, including wiring, network, connection process, and security requirements that are intended to lead to appropriate authorities to operate (ATOs).

DoD continues to make progress on the requirements that were levied under the Fiscal Year (FY) 2020 National Defense Authorization Act (NDAA) Section 847, regarding Foreign Ownership Control, and Influence (FOCI) assessments.

Mr. Spinnanger mentioned the ongoing issue regarding Joint Ventures (JV) and Facility Security Clearance (FCL) requirements. There was a provision or there's a provision in the FY 2022 NDAA, Section 1629, which states that if both entities that form a JV are cleared, the JV company itself does not require a facility clearance. In order to address Section 1629 language, DoD is intending to publish a directed type of memorandum to provide guidance on JVs that had been awarded via declassified contracts. There's similar language in the Small Business Administration (SBA) federal rule published in late 2020 that DoD believes must be addressed in this regulation and guidance.

Ms. Jennifer Aquinas from Air Force discussed the Joint Ventures. They were able to issue a classified contract to an uncleared JV and allow performance on a contract without a facility clearance, however, the regulatory conflict remains between the SBA and the NISP. At the last NISPPAC meeting, ISOO advised that the SBA rule was not intended to remove the facility clearance requirement. ISOO is still working on a notice that will clarify the issue.

Mr. Keith Minard provided an update from DCSA. DCSA has a new Deputy Director, Mr. Daniel Lecce, and a new Industrial Security Director, Mr. Matthew Redding. DCSA has returned to onsite assessments and personnel are out in the field onsite doing security reviews. DCSA is now working with all action officers to look at items that can change, and how it can improve, while investigating best practices that came out of last year's implementation of the NISPOM.

The amendment to 32 CFR Part 117, deferring the reporting of Security Executive Agent Directive (SEAD 3) foreign travel requirements for 18 months from the issuance date will begin in August of this year. Part of this was the ability for Industry to bulk upload foreign travel, rather than doing one-by-one submissions of foreign travel, to try to better enable the reporting requirements and ease some of the strain.

The SEAD 3 frequently asked questions were revised on the DCSA website. Along with that, the staff created an intuitive tool that helps Industry walk through the types of contact reporting required by SEAD 3. DCSA also posted a short on security in-depth. Six and eight-minute slides are narrated for easy use and information updates.

Ms. Valerie Kerben, Chief, Policy & Collaboration Group, Special Security Directorate, National Counterintelligence and Security Center (NCSC), Office of the Director of National Intelligence (ODNI) provided an update on Security Executive Agent (SecEA) policies. The Transforming Federal Personnel Vetting cabinet memorandum was signed by the National Security Advisor, Jake Sullivan, on December 14, 2021 and issued to the Executive branch.

Three Trusted Workforce guidelines were signed by ODNI as the Security Executive Agent and Office of Personnel Management (OPM) Director as the Suitability and Credentialing Executive Agent, which

describe the outcomes for successful personnel vetting programs. Namely, Federal Personnel Vetting Guidelines, the Federal Personnel Vetting Engagement Guidelines and the Performance Management Guidelines in Jan 2022.

Another policy that clarified and outlined adjudicative guidance on the recreational use of marijuana, the use of CBD products and the investments of marijuana-related businesses, was signed and issued by the SecEA on December 21, 2021. ODNI will be issuing new Federal Vetting Investigative Standards and a new SEAD 9 - titled Whistleblower Protection: Appellate Review of Retaliation Regarding Security Clearances and Access. It is the whistleblower protection appellate review of retaliation regarding security clearance. ODNI is just finishing up coordination and adjudication on this.

Mr. Richard DeJausserand, Deputy Director of the National Security Services Division at the Department of Homeland Security (DHS) provided the DHS update. The agency continues the implementation of Trusted Workforce 2.0. To date, DHS has enrolled about 83% of the security population into the ODNI Continuous Evaluation (CE) system and are on track for full implementation by FY 2024. The insider threat and personal security teams continue to work together to develop policy and Standard Operating Procedures (SOPs) and are meeting once a month.

Ms. Natasha Sumter, Office of Security Policy, Department of Energy (DOE), provided the DOE update. DOE has been reviewing order 470.4B, DOE's Safeguards and Security Program Order. This order handles or discusses much of the industrial security matters found in the NISPOM or the 32 CFR 2004. DOE is currently beginning the process to open that order for a complete rewrite. The agency has also reviewed 32 CFR 2002, and have implemented that regulation via DOE Order 471.7, which is Controlled Unclassified Information (CUI), which was published February 3, 2022. DOE policy 226.2, Policy for Federal Oversight and Contractor Assurances and DOE Order, 226.1B, Implementation of the Department of Energy Oversight Policy provide the oversight structure for both federal operations and contractor assurances.

Mr. Denis Brady from the Nuclear Regulatory Commission (NRC) provided the NRC update. NRC has their CUI policy statement published and the rule has been approved by their commission that supports the NRC's transition to CUI September 2022.

Felicia from the Central Intelligence Agency (CIA) provided their update. In reference to NISPOM implementation, the CIA Industry Security staff is actively engaged in the implementation of the new NISPOM as a federal rule. They are also incorporating SEAD 4 updates into the current policy. Regarding CUI, they are working closely with the ODNI and representatives. CIA is actively participating in multiple government-led working groups focused on providing substantive comments and review of Trusted Workforce 2.0 draft policy.

Mr. Robert Mason, alarm system auditor and Underwriters Laboratory, LLC (UL 2050) subject matter expert with UL, presented a briefing on the four types of alarm monitoring. The first monitoring of the standard is a government contracting monitoring stations. It is a government contractor location that can monitor UL 2050 certificates within a 24 hour radius from that location. The alarm service company that issues the certificate also must maintain the receiving equipment at the monitoring station. The second monitoring is a national monitoring industrial station, and they can monitor outside those 240 miles and a four hour radius from the station. The third option for monitoring these types of certificates are a central commercial UL listed station. The fourth type of monitoring is law enforcement.

General Services Administration (GSA)'s Chief of Policy Standards and Engineering Branch, Mr. Chris Pollock gave an update on safe ordering. First, if there is the requirement to store classified information within the contract, that will be in the DD254. There needs to be a Department of Defense Activity Address Code (DoDAAC). These are assigned by the government contracting officer. GSA allows payment via different methods, including PayPal, bank accounts, or credit cards. It is critical that manufacturers have a point of contact to be able to work through any issues that arise.

The cost of steel is up about 200% since March of 2020. GSA has also been affected by the shortage of electronic components which has caused some redesign and retesting and additional costs for locks. This has resulted in about a 30-40% increase in the cost of GSA approved containers. GSA tries to maintain a 30-45-day delivery time in contracts, but during COVID, that time slipped sometimes as far as 90 days, but they are working to get back to the 30 day timeframe.

There appears to be confusion with ISOO Notice 2021-01, Rescinding Approval of Pre-1989 General Services Administration (GSA)-Approved Containers. The best resource to find out information is the DoD Lock Program, https://exwc.navfac.navy.mil/DoD-Lock-Program/, which is available to both government and Industry.

Mr. Greg Pannoni gave the update for the Clearance and NISPPAC Information Systems Authorization (NISA) working groups. He discussed the SF312 non-disclosure agreement allowing for digital signatures. ISOO coordinated this form with ODNI, as well as the Department of Justice (DOJ). May 9, 2022, 32 CFR Part 2001 will be amended.

He also discussed ISOO's reform on collecting data for the Annual Report to the President. One of the things ISOO has been looking at besides the overall data reform initiative for collecting information is cost. There are requirements in two Executive Orders (NISP, CNSI)that concern cost. ISOO has been meeting with Government to discuss a way to get better estimates of the cost under the NISP. DOD put forward an outline that captures both the major buckets of costs that will impact Industry, which is being discussed with the other CSAs as well. The government will share this information with Industry once it is ready to be shared.

There is a concern with the processing time and rejection rate for facility security clearances (FCLs). It was recommended to form a small ad hoc working group, and for the chair to focus on the key issues. The group could focus on the major impediments that are causing this rejection rate. Also, the group could focus on the FOCI aspects of clearing the entity.

Heather Sims reminded Industry that if there is an unfunded requirement or a new process change after the contract has been awarded, to go back to the government customer and renegotiate that contract. She also mentioned that during the Joint Personnel Adjudication System (JPAS), DISS and National Background Investigation Services (NBIS) transition, Industry absorbed a lot money and resources when they corrected that data.

Mr. David Scott gave the briefing for DCSA. The regions have been realigned. In December, there was a process in which DCSA could change a workflow and package the workflow. Due to the strong relationship with the NISA Working Group, they were able to collaborate, and communicate effectively to make a change in January. It happened in January with zero downtime and Industry was fully engaged.

There have been some concerns with access to Enterprise Mission Assurance Support Service (eMASS) computer-based training which is now hosted in the Risk Management Framework (RMF) knowledge service. DCSA has been working with the Defense Information Systems Agency (DISA), and recently got approval to host in the step environment from Center for Development of Security Excellence (CDSE). They are working on that issue at the present time. As soon as they get approval to hit the live system they will work with the NISA working group to publicize that.

Another positive engagement is with the NISP connection process guide. This guide is instrumental in providing a hands-on process flow for any contractual requirement to interconnect with a system within the NISP. Due to the collaboration with the NISA working group, DCSA received a lot of feedback over the course of the last three months. They are looking to formally publish that feedback through the processes of the federal registry.

DCSA will continue eMASS updates and job aids and will utilize eMASS as their help desk page to put information out to Industry as fast as possible to all 4,000 users. They are also working internally on an update overall DAAPM 3.0 and will partner with the NISA working group to close any gaps in processes and the procedures that industry observes. For the Command Cyber Readiness Inspections, DCSA has already executed one and is already planning for the rest of FY 2022 to conduct many more.

Ms. Donna McLeod, DCSA, provided the vetting statistics for DCSA. For VRO (Vetting Risk Operations), the investigation submission and interim industry populations are approximately a million. 90% of all initial investigations have an interim determination made on average within five to seven days.

DCSA reached full enrollment of DoD cleared population into a trusted workforce CV compliance program in FY 2021 and continue to work the set to a steady stay of new enrollments. Criminal issues and financial issues are the most common valid actionable alerts received. The discussion moved onto the background investigation. The total inventory for background investigation continues to remain within a stable state.

DCSA is largely meeting Industry adjudication timeliness goals with a few exceptions. The top three reasons personnel are being denied or revoked remain financial considerations, criminal conduct, and personal conduct. Industry inventory has been relatively steady for the last four quarters and they closed approximately 94,000 cases this year.

Mr. Paul Dufresne provided an update for DOE. The DOE has been meeting the 20-day standard for the adjudications on initial investigations, as well as the 30 days on the re-investigations. For T3 investigations over the last 12 months, they have been meeting the Intelligence Reform and Terrorism Prevention Act (IRTPA) standards.

Mr. Erich Person from the DOE gave an update on Insider Threat Office initiatives. The Insider Threat Program includes revising DOE order 470.5.

Mr. Chris Heilig, Chief of the Personnel Security Branch at the Nuclear Regulatory Commission (NRC), provided the agency update. They are TW 1.25 compliant and working actively with DCSA to meet the 1.5 compliant deadline at the end of this fiscal year.

Mr. Perry Russell-Hunter, from the Defense Office of Hearings and Appeals (DOHA) provided their update. He recognized Greg Pannoni for his over four decades of exemplary public service to the NISP

and to the nation. DOHA is still making maximum use of telework, except for the personnel who are conducting and supporting the in-person hearings that are a core part of the DOHA mission. They are fully masked at all times in all hearings and employ a full range of safety precautions in those hearings and in the office. Statements of Reasons (SORs) are still going out in typical numbers and are timely, with 257 SOR reviews currently pending. That number is within the typical on-hand SOR review workload.

DOHA reviewed a typical average of 2,600 SORs per year pre-pandemic. In Fiscal Year 2021, DOHA legal reviewed and revised 3,021 SORs. In the calendar year 2021, DOHA reviewed 2,578 SORs. DOHA has kept up with all of the draft SORs sent by the DoD CAF for legal review and worked at a typical operating pace, despite the pandemic, using DoD SAFE to ensure a secure workflow.

The next NISPPAC is scheduled for November 2, 2022. All NISPPAC meeting announcements are posted in the federal register at https://www.federalregister.gov/ approximately 30 days before the meeting, along with the ISOO blog at https://isoo-overview.blogs.archives.gov/.

Summary of Action items

ISOO will continue working on the issuance of a notice on joint ventures.

Industry Spokesperson will form an ad hoc working group to discuss concerns and questions regarding the rejection rate and processing time for entity eligibility determinations, i.e., facility clearances.

Questions and Answers from the NISPPAC

Q: How can I reach out to NISPPAC Industry?

A: nisppacindustry@gmail.com.

Q: How do companies get a DoDAAC in order to order a GSA approved container for storage of classified information?

A: The assignment of the DoDAAC has to be accomplished by the Government Contracting Officer. Any subcontractor who needs to order a GSA Approved container will need to work back through the prime contractor to the contracting officer.

Q: Multiple companies who produce and sell GSA-approved containers (I assume on a direct GSA contract) are still quoting them for Industry and fulfilling orders. How is this possible, if we are required to procure directly through GSA? If a container is purchased in this manner, what are the concerns/ consequences?

A: In general, the GSA approved contract holders should not be fulfilling orders for the GSA approved containers outside of the GSA ordering system. There are a few exceptions where specific permission is given based on the specific situation however.

Be aware that there are some companies attempting to sell used or refurbished GSA approved containers. These should never be used to store classified information (See ISOO Notice 2012-04).

The Government cannot limit or control the communication between one private company and another.

Consequences for not following requirements for protecting classified information can be severe.

NISPPAC Attendance

Abba, David
Abbott, Aprille
Abella, Eric
Adam, MacVean
Adams, Kendall
Aden, Casey
Adissu, Mekdes
Adkins, Ronnie
Aghdam, Laura
Ahad, John
Akers, Lynetta
Albalos, Raven
Albertini, Wendy
Alexander, Christine
Allen, Nicole
Alvarez, Damien
Ambrose, Zorica
Andablo, Yvette
Andrade, John
Andrews, Kathy
Anello, Tonya
Apostol, Amy
Aquinas, Jennifer
Arbelo, Albert
Arbuckle, Leslie
Archibeque, Norbert
Arffman, Kathryn
Argumedo, Lori
Armstrong, Deborah
Arriaga, Dennis
Ashby, Holli
Ashley, Janet
Auman, Jenna
Babic, Adriana
Backhus, Annie
Bailey, Benny
Barnes, Sean
Barnhart, Jason
Baros, Tracy
Barry, John
Bastien, Addie
Bate, Kelly
Baugher, Kimberly
Beaghley, Sina
Beasley, Michelle
Belcher, Lara
Bell, Jordan
Bellagamba, Barbara
Belsinger, Deborah
Bergamini, Margaret
Bergeman, Stephen
Berry, Kathleen
Bethea, Nasu
Bird, Ryan
Black, Christina
Black, Laura
Blackburn, Cindy
Bland Jr., Booker
Blazic, Andrew
Bledsoe, David
Blount, Richard
Boaz, Jennifer
Boccalino, Michael
Bock, Kristy
Bodrick, Detra
Boettcher, Collin
Boley, Jan
Boling, Daniel
Bongiorno, Nick
Boomer, Mindy
Borland, Jennifer
Borrero, Rosael
Borrero, Rosie
Bosch, Lucas
Bostjanick, Stacy
Botteicher, Joshua
Boucek, Jacob
Bouchard, Ross
Bowman, Jennifer
Brackens, Jennie
Bradley, Mark
Brady, Denis
Brain, Steven
Brandt, Elizabeth
Brauer, John
Britt, Martin
Broer, Anja
Brokenik, Trish
Brooks, Beverly
Broussard, Derrick
Brown, Jennifer
Brown, Kelly
Brown, Robert
Brown, Shannon
Brown, Shawna
Brumfield, Lisa
Bryan, Karen
Bryan, Phyllis
Buckingham, Jon
Budd, Quinetta
Burger, David
Burke, Harold
Burnett, Karen
Burns, Lynn
Burrell, Gerome
Burris, James
Busa, Theresa
Busch, Melissa
Bush, Seth
Bynum, Mark
Byrge, David
Cabe, John
Cagney, Megan
Call, Samantha
Callier, Jewel
Carey, Jill
Carlyon, Michelle
Carnaghi, Suanne
Carpenter, Allison
Carpenter, Marcus
Carpenter, Terry
Carter, Gari
Carzo, Frank
Cattaneo, John
Cavalier, Sarah
Cavano Sr., Jeffrey
Cecere, Art
Ceol, Edward
Chandler, Tammy
Charyton, Dianne
Chavez, Steven
Cheeks, Mark
Chituras, Jimmie
Christian, Laurie
Chung, Kuk
Chupka, Matthew
Chvotkin, Alan
Cippel, Melissa
Clader, Heather
Clagett, James
Clancy, Jamie
Clark, Jerry
Clark, Larry
Clasen, Melissa
Clifford, Debra
Cole-Tate, Deborah
Collins, Randi
Collo, Robin
Condon, Jessica
Conley, John
Connelly, Michael
Connerley, Christopher
Cook, Krista
Cooke, David
Coonce, Julie
Cooper, Jonathan
Cooper, Nicole
Corbin, Christopher
Crabtree, Misty
Craft, Linda M
Craig, Diane
Crew, Kimberly
Cronin, Scott
Crosby, Kristin
Croson, Matthew
Culver, Terry V.
Cunningham, Phillip
DaFermo, Mary
Damerow, Shawyn
Daniels, Sharlene
Danielson, Krista
DAnthony, Stacey
Daugherty, Linda
Davenport, Amanda
Davidson, Mathew
Davis, Amy
Davis, Claris
Davis, Darrell

Davis, Glynn
Davis, James
Davis, Mary
Dawson, Steven
de la Garza, Nancy
Deabler, Angela
Dean, M.C.
Dean, Mary
DeCastro, Orlando
Deely, Maura
Deen, Christina
Dejausserand, Richard
DeJesus, Matthew
Demers, Michael
DeMong, Jeremy
Denegal, Robert
DeSousa, David
Devers, Travon
Diacoumis, Ted
DiazMartinez, Sarah
Dimeler, Jenifer
Dinkel, Jane
Dockins, Michelle
Dodson, Jeffrey
Doherty, Jennifer
Donahay, Joseph
Donnelly, Janet
Dotson, Virgil
Doubleday, Justin
Dragan, Chad
Driscoll, Michael
Drummond, Fred
Dubay, Greg
Dublin, Scott
Dubuque, Katja
Dufresne, Paul
Dunbar, Brian
Dupnak, Michael
Dupre, Jacqueline
Durkin, Tracy
Duvall, William
Dwyer, Dustin
Eanes, Matt
Eckel, Mark
Eckerstrom, Suzanne
Eckert, Ed
Eddins, Kristina
Edge, Kimberly
Edington, Mary
Edmonds, Tracy
Edwards, Douglas
Edwards, Kimberly
Egan, Amanda
Elliott, Tanya
Embree, Peter
Empeno, Henry
England, Michael
Enriquez, Marcus
Errington, Gordon
Escobar, Jose
Escobar, Michael
Escobar, Sheri
Escobedo, Robert
Eshman, Craig
Eskelsen, Jon
Eury, Laura
Exile, Samuel
Fadden, Geraldine
Farina, Nicole
Fehlner, Scott
Feldman, Ben
Felicia
Fell, Rob
Fenger, Joel
Ferrell, Andrea
Finklea, Anthony
Fisher, Darci
Fitch, Zachary
Fitz-Enz, Jonathan
Flaherty, Joann
Emma
Fleeger, Daniel
Flores, Darrell
Focht, Jason
Foran, Peter
Forbregd-Gossage, Devin
Franklin, Broderick
Frederick, Kellyd
Freeman, Lisa
Freestone, John
Frisbey, David
Frownfelter, Mark
Funicello, Kasey
Funicello, Lorena
Fuster, Kathleen
Gabeler, Jennifer
Gander, Alysa
Garcia, Orlando
Garcia, Paul
Garcia, Rogelio
Gardner, Kelly
Garland, Sheila
Garner, Byron
Garner, Carol
Garvin, Kelly
Gass, Audra
Geisler, Angela
Gerlich, Chris
Ghannam, Samie
Gibbs, Jennell
Gibbs, Katrina
Gibbs, Katrina
Giese, Steven
Gillespie, Ellen
Girven, Richard
Gladney, Jeanine
Glassic, Scott
Gleason, Kimberly
Gnanamurthy, Kumar
Goldberg, Jeffrey
Goldsmith, Alison
Goldstein, Donald
Gonchar, Cole
Gonzales, Eva
Goodwin, George
Graham, Jennifer
Gray, Juaquita
Gray, Tonya
Greaver, Angela
Green, Heather
Greene, Gus
Griffin, Diane
Griffin, Katherine
Griffith, Noelle
Grimes, Daniel
Grossman, Amy
Guarrasi, Peter
Guatemala, Christina
Guerrero, Marcia
Gurman, Nina
Gutierrez, Jessica
Hagenbuch, Chris
Haire, Tamara
Haley, Rene
Halfhill, Heather
Halk, Adam
Hall, Brent
Hall, John
Hall, Kevin
Hamann, Donald
Hamilton, Pamela
Hand, Emily
Hanson, Kai
Harbison, Patrick
Hargis, Jeremy
Harkema, Scott
Harmon, Joshua
Harne, Joseph
Harper, Taylor
Harris Pagán, Heather
Harris, James
Harsch, Stephen
Hassebrock, Douglas
Hawk, Jason
Hawthorne, Michael
Hayes, Robert
Hazen, Scott
Heaton, Pamela
Heikkinen-Trone, Susan
Heil, Valerie
Heilig, Chris
Heine, Nichole
Helstowski, Emily
Helton, Alicia
Henderson, Alexis
Henderson, Kaila
Henderson, William
Hensley, Michael
Hertzog, Conrad
Hewlett, Daisha
High, Howard
Hill, Brett
Himelright, Todd

Hinds, Charles
Hodges, Hope
Hogan, Teresa
Holderman, David
Holland, Stephen
Hollandsworth, Matthew
Hollingsworth, Danielle
Holloman, Noelle
Holmberg, Brandon
Hommer, Michael
Honeyman, Susan
Hood, Jennifer
Hoover, Ronald
Howar, Laura
Howard, Kedrick
Howe, Thomas
Howell, Eric
Howell, Mark
Huber, Donna
Hubert, Alexander
Hughes, Janet
Hughes, Rachel
Hulet, Michael
Hunt, Matthew
Husker, Frank
Illidge, Kaitlin
Immel, Christopher
Isaac, Mary
Izadi, Katayoun
Jacqueline, Shular
Jamaldinian, Rafiq
James, Steven
Jarvie, Vincent
Jefferson, Felicia
Jenkins, LeeAnn
Jensen, Kathryn
Jiggetts, Lauren
Jimenez, Elizabeth
Johnson, Ashley
Johnson, Regina
Johnson, Troy
Johnson, Tyler
Jolls, Robert
Jones, Adam
Jones, Caleb
Jones, Cecilia
Jones, Derek
Jones, Derick
Jones, Kenneth
Jones, P Quinnatt
Jones, Russell
Jones, Tara
Jones-McGee, Darius
Jonsson, Agust
Jordan, Margaretanne
Jordan, Yvonne
Juni, Daniel
K, Kamila
Kahn, Shanna
Kalman, Eric
Kaohi, Catherine
Kaveney, Brian
Kay, Susan
Keller, Katie
Kelly, Michael
Kennedy, Beverlee
Kennedy, James
Kepley, Kay
Kerben, Valerie
Kerr, Julie
Kerr, Robert
Kester, James
Kidd, Linda
Kieschnick, Lorreen
Killian, Joseph
Kimball, Mary
King, Scott
KingRatzel, Betty
Kipp, Steven
Kirby, Jen
Kirby, Jennifer
Kitts, Karen
Kitzman, Matthew
Klaczyk, Joseph
Klein, Fred
Klem, Jeremy
Klink, Carolina
Knight, Richard
Knox, Daniel
Kobus, Jason
Kocher, Charles
Konicki, David
KoslowVerdi, Alison
Kraus, Joseph
Kroeplin, Mark
Kutchak, Nicholas
LaBeach, Stephanie
Lambert, Brett
Lambert, Erin
Lang, Matthew
Langer, Thomas
Laperle, Deanna
Latal, Connie
Lau, Amanda
Lawson, Pamela
Laybourne, Krista
Layne, Karen
Leake, Melissa
Lecce, Daniel
Lee, Jennifer
Lee, Jessica
Leonard, Chris
Levasseur, Nicholas
Levett, Mark
Lewis, June
Lewis, Natasha
Lewis, Tiffany
LHeureux, Ann Marie
LHeureux, Lawrence
Lietzau, William
Lilly, Chris
Limon, Katherine
Lindsey, Joseph
Linthicum, Tim
Lochli, Andrew
Logan, JessYvonne
Logan, Julia
Londregan, Michael
Long, Jamie
Lopez, Charles
Lord, Ginger
Lorenz, Lori
Lotwin, Andrew
Lowry, Ashley
Lowy, David
Lucas, Mark
Lucero, Christopher
Lucock, Cynthia
Luera, Xanne
Lundquist, Peg
Lupo, Tracy
Ly, Daniel
Lynch, Sammy
Lyons, Ashley
Macey, Christopher
MacKenzie, Cynthia
Mackey, Brian
Mackey, Marvin
Mackey, Shelton
Macwan, Christopher
Mahoney, Collin
Malbone, Nicole
Malone, Paul
Mammana, Gregory
Mancini, Scott
Mangum, Jon
Manley, Crystal
Manning, Alexis
Manning, Lesa
Mannix, Brian
Marino, Craig
Marino, Keith
Marks, Michael
Marsh, James
Marshall, Ezekiel
Martens, Sheri
Martin, Christina
Martin, Kenneth
Martin, Price
Martineau, Marianna
Martinez, Deborah
Martinez, Elias
Martinez, Hazel
Mason, Bob
Massaro, James
Masse, Todd
Matthews, Will
Mattox, Lisa
Mayercin, Elizabeth
Mayuga, Jonathan
Mazanec, Jeffrey
McCaffrey, Mary Rose
McCarthy, Kevin

McCarthy, Leslie
McCausland, Ryan
McCloud, Adrienne
McCoy, Linda
McDonnell, Bridget
McDowell, Heather
McGarvey, Daniel
McGowan, Edward
McKay, Kyle
McLaughlin, Schuyler
McLeod, Donna
McLeod, Risa
McMillan, Sean
McNichol, Lindsey
McQuiston, Russell
Means, David
Measures, Lisa
Mechem, Stormie
MedinaCreel, Tina
Meek, Eric
Meier, Scott
Mencin, Brett
Metcalf, Jessica
Meyer, Nick
Michaud, Jean
Michelle Madison
Miller, David
Miller, Erik
Miller, Kevin
Miller, Lisa
Milligan, Aaron
Mills, Katherine
Minard, Keith
Minard, Verna
Mitchell, Bruce
Mittleman, Elaine
Molnar, Kimberly
Moore, Kathleen
Morales, Albert
Morgan, Justin
Morris, Christine
Morrison, Robert
Morton, Tracy
Moseley, Paula
Moshos, Phyllis
Mosier, Jennifer
Moss Jr., Leonard
Moss, Lesya
Motelet, Michelle
Mullen, Ryan
Mumford, Gregory
Murphy, Tyler
Nascembeni, Carlo
Neale, Cynthia
Needle, Kandace
Nencioni, Natalie
Nick, John
Nickel, Robin
Nikolaus, Suzanne
Nio, Chuck
Noles, Chad
Norman, Diane
Norman, Wayne
Norris, Alison
Nunn, SeKitha
O Halloran, Jennifer
O'Brien, Jason
O'Kane, Elizabeth
Olson, Brian
Omo, Stacey
Onusko, Jim
Opilla, Hunter
Oppenhagen, Christine
Orlando, Michael
O'Rourke, Frances
Orr, Mary
Orsini, Mario
Osmer, Carlene
Ososkie, Charles
Overby, Andrew
Palmar, Jose
Pannoni, Gregory
Pappas, Joyce
Parker, Andrew
Parr, Doris
Pashoian, Norman
Patterson, Casandra
Patterson, Jennifer
Paul, Kristin
Payne, Daniel
Pearson Lloyd, Laurel
Pekrul, Mark
Pendleton, Brandi
Persavich, Alex
Person, Erick
Pettengill, Chantel
Peykar, Rambod
Phagura, Satminder
Phalen Jr., Charles
Phelps, Devon
Pherson, Katherine
Phillips, Terry
Pickard, Angela
Pickering, Tamiko
Plummer, Raenell
Pollock, Christopher
Pontiakos, Michael
Porter, Dara
Porter, Lizet
Power, Kyla
Praeger, Derek
Prevost, Jacquelyn
Price, Janel
Price, Joyce
Pritchard, Gregory
Proctor, Joan
Proia, Amanda
Propst, Linda
Provencher, Marguerite
Pueschner, Todd
Pulliam, Donna
Pyles, Larry
Quarles, Darren
Queen, Clayton
R, N
Raju, Clara
Randall, Sheila
Rankin, Kelli
Rasmussen, Jeremy
Ray, Michael
Ray, Richard
Razumovsky, Andrew
Re, Nicolas
Reardon, Amy
Reck, Sydney
Redding, Matthew
Reding, David
Reid, Garry
Reidy, Lisa
Reneski, Christine
Renzella, Allyson
Rice, Jo
Richardson, Daniel
Richardson, James
Richardson, Linda
Riches, Dan
Riddle, Samantha
Riener, April
Ritter, Michael
Rivers, Isaiah
Robison, Amanda
Rocha, Treva
Roche, Matthew
Rodowsky, Laura
Rodriguez, Chamagne
Rodriguez, Jessica
Rodriguez, Rigoberto
Rogers, Geraldine
Rogers, Whitney
Rojas, Rachel
Rommal, Eric
Ronyecs, Laurie
Rosenwasser, Jon
Rosera, Stephen
Ross, Stephanie
Rossignol, Ryan
Roswal, Andrew
Ruffini, Julia
Ruiz, Kimberly
Ruiz, Ray
Ruizno, Kelvin
Russ, Lee
Russ, William
Russell-Hunter, Perry
Rust, Daniel
Sadler, Greg
Saloom, Charles
Samuels, Al
Sanchez, Sunni
Sandlin, Taylor
Sangobowale, Sam
Sargent, Patrick
Sata, Dana

Savoy, Shayla
Schellenschlager, Cherin
Schermacher, Cari
Schmidt, Loren
Schneider, William
Schneider, Sandra
Schneider, Scott
Schoenig, Caitlyn
Schultz, Joe
Scott, Christopher
Scott, David
Scott, James
Scottorn, Lisa
Scovel, Yen
Sease, James
Seay, Tracy
Seiler, Jason
Senutovitch, Diane
Settles, Christina
Shade, Karl
Shaffer, Laura
Sharpe, Suzanne
Shaw, Melissa
Shaw, Richard
Sheridan, Brian
Sherwin, Mark
Shier, Max
Shimamura, Judy
Sickmond, Stephanie
Sims, Christopher
Sims, Heather
Singh, Kulvinder
Singletary, Patrice
Sivak, Tracy
Sjodahl, Debbie
Skinner, John
Slinko, Luke
Sloan, William
Smick, Martha
Smith, Anthony
Smith, Crystal
Smith, Kyle
Smith, Linwood
Smoot, Teresa
Sobocinski, Jon
Soriano, Rojohn
Sowa, Robert
Sowell, Charles
Speace, Garrett
Spencer, Chuck
Spinnanger, Jeffrey
Stambaugh, Christine
Standifer, Karla
Stanley, Terence
Stayton, Kelley
Steinbuch, Michael
Stellflug, Michelle
Stelling, John
Stephens, Brooke
Stern, Steven
Steudlein, Steven
Stewart, Patti
Still, Tonya
Stolkey, Christopher
Stone, Alissa
Stone, Cheryl
Streeter, Frankie
Strid, Jimmy
Struttmann, Michael
Stubbs, Marguerite
Stutts, Anna Kirsten
Sublett, Kent
Sullivan, Caolinn
Sullivan, Patrick
Sulzer, Alexandria
Sumpter, Valerie
Sumter, Natasha
Sutphin, Michelle
Swinburne, Jessica
Switala, Jamie
Szady, David
Szewc, Stephen
TaftMoore, Dianne
Taimassov, Alexandre
Talley, Thomas
Tate, Charles
Taylor, Chalyndria
Temple, Brenda
Terreri, Eric
Theriault, Jason
Thibault, Crystal
Thoma, Jeffrey
Thomas, Doug
Thomas, MaryJo
Thompson, BLinda
Thompson, Donna
Thompson, Robert
Thornton, Diana
Thornton, Tracy
Timm, Jason
Torres, Gregory
Tostado, Thomas
Tran, Kat
Tringali, Robert
Trinidad, Jeff
Trono, Robert
Trudel, Mark
Tucker, Bruce
Tucker, Joni
Tunell, John
Turke, Zachary
Turner, Shawntelle
Ullmann, John
Vaccariello, Jeffrey
Valencia, Juan
Van Hook, Donna
Van Le, Phuoc
Vargas, Tony
Vaughan, Tom
Vaughn, Susie
Vaughn, William
Vetra, Mike
Vincent, Jennifer
Vincent, Larry
Vitoritt, Hanni
Vrahnos, Michael
Vucci, Blane
Walker, Sharese
Wall, Thomas
Wallace, Charlene
Walsh, Justin
Ware, Laura
Waters, Timothy
Watkins, LaTasha
Watters, Michelle
Weatherby, Bradley
WeaverLillard, JoAnda
Webber, JoAnn
Webster, Anzio
Wehner, Derrick
Weldon, Stephen
Wendell, Jeremy
West, Janell
Wever, Scott
White, Iryna
Whitehead, Lynette
Whitley, Stephanie
Whitteker, Mark
Wible, Bradford
Wiesner, Todd
Wilder, Christy
Wilkes, Quinton
Williams, Alyson
Williams, Angela
Williams, Candace
Williams, Daniel
Williams, Elizabeth
Williams, Jennifer
Williams, Kristin
Williams, Margaret
Wilson, Bryan
Wilson, Kenisia
Wilson, Trista
Win, David
Winford, Donneaka
Winn, Terrance
Winningham, Amy
Winston, Robert
Wisnosky, Roger
Wojcik, John
Wolf, Mindy
Wood, Delvin
Woolf, Michael
Woolheater, Dale
Woolsey, Wailohia
Worsham, Robert
Wright, Paula
Yenigun, Katie
Yocum, Patrick
Young, Ronald
Zenkewicz, Scott
Ziebell, Krista
Ziesmer, Richard
Ziesmer, Rick
Zweil, Alison

National Industrial Security Systems (UL 2050) 5th Edition November 5, 2010

National Industrial Security Program Policy Advisory Committee
April 27, 2022

Empowering Trust®

Government Contractor Monitoring Station

A monitoring station that is operated by a defense contractor with the purpose of monitoring Industrial Security Systems that are installed in areas occupied by that defense contractor or subcontractors. The alarm service company that maintains the certificated alarm systems are required to verify compliance with UL2050. The systems that are monitored by a GCMS are required to be within 240 miles of the GCMS location. Systems that exceed 240 miles will require a NIMS listing.

Government Contractor Monitoring Station

A National Industrial Security System involves alarm detection equipment installed at a protected premise and may be remotely monitored on alarm-receiving equipment located at a Government Contractor Monitoring Station. The Government Contractor Monitoring Station shall comply with the fundamental requirements as specified in UL 2050

Government Contractor Monitoring Station

The following are the fundamentals for a GCMS to comply with UL 2050:

- Physical Protection
- Alarm Receiving Equipment
- Fire Protection
- Clocks
- Primary and Secondary Power
- Communication Circuits
- Personnel

Government Contractor Monitoring Station

The following are key areas of protection service that are provided by a GCMS:

- Monitoring of Alarm Systems
- Openings and Closings
- Alarms and Unauthorized Openings
- Dispatching Investigators
- Trouble Signals and Service Calls
- Creation of Records

National Industrial Monitoring Station

A monitoring station operated by a defense contractor or central station that are providing monitoring services for National Industrial Security Systems which are more than 240 miles away from the station.

National Industrial Monitoring Station

A National Industrial Security System involves alarm detection equipment installed at a protected premise and may be remotely monitored on alarm-receiving equipment located at a National Industrial Monitoring Station. The National Industrial Monitoring Station shall comply with the fundamental requirements as specified in UL 2050.

National Industrial Monitoring Station

The following are the fundamentals for a NIMS to comply with UL 2050:

- Physical Protection
- Alarm Receiving Equipment
- Fire Protection
- Clocks
- Primary and Secondary Power
- Communication Circuits
- Personnel

National Industrial Monitoring Station

The following are key areas of protection service that are provided by a NIMS:

- Monitoring of Alarm Systems
- Openings and Closings
- Alarms and Unauthorized Openings
- Dispatching Investigators
- Trouble Signals and Service Calls
- Creation of Records

Commercial UL Central Stations Provide

A National Industrial Security System involves alarm detection equipment installed at a protected premise and may be remotely monitored on alarm-receiving equipment located at Central Stations. The UL Central Stations shall be listed under the UUFX (Fire), CPVX (Burglar), or CVSU (Residential Monitoring).

Commercial UL Central Stations Provide

The following are key areas of protection service that are provided by the UL stations:

- Monitoring of Alarm Systems
- Openings and Closings
- Alarms and Unauthorized Openings
- Dispatching Investigators
- Trouble Signals and Service Calls
- Creation of Records

Law-Enforcement Agency

A National Industrial Security System involves alarm detection equipment installed at a protected premise and may be remotely monitored on alarm-receiving equipment located at a Law-Enforcement Agency. The Law-Enforcement Agency shall comply with the fundamental requirements as specified in UL 2050.

Law-Enforcement Agency

The following is the basic fundamental for a Law-Enforcement Agency to comply with UL 2050:

- Alarm Receiving Equipment

The following are key areas of protection service that are provided by a Law-Enforcement Agency:

- Monitoring of Alarm Systems
- Alarms and Unauthorized Openings
- Dispatching Law-Enforcement Person
- Trouble Signals and Service Calls
- Creation of Records

UNDERWRITERS LABORATORIES INC. CERTIFICATION REQUIREMENT DECISION

This Certification Requirement Decision is prepared and published by Underwriters Laboratories Inc. (UL). It is normative for the applicable UL Product Certification Program(s); however, it is currently not part of the UL Standard(s) referenced below.

Product Category (CCN): CRZH & CRZM
Standard Number: UL 2050
Standard Title: National Industrial Security Systems
Edition Date: November 5, 2010
Edition Number: 5
Section / Paragraph Reference: 6.16.2 & 6.16.3
Subject: Communication Infrastructure

DECISION:

The additional paragraphs 6.16.2 and 6.16.3 provide redundancy for the Government Contracting Monitoring Stations (GCMS) and National Industrial Monitoring Stations (NIMS) when using an automation system.

6.16.2 If the central station receives signals from monitored alarm systems that are transmitted with either a packet switched data network or a managed facilities based voice network the station shall utilize communication services that deliver geographically diverse signal pathways, if possible by:

a) Utilizing two independent internet service providers (ISP) or two independent managed facilities based voice network (MFVN) providers or;

b) Utilizing one internet service provider (ISP) or one managed facilities based voice network (MFVN) provider that provides contracted diverse signal pathways arranged so that the pathways are not likely to be affected by the same natural or man-made disasters or single point of failure.

6.16.3 If the central station utilizes managed facilities based voice network (MFVN) for voice telephone communication, the station shall utilize communication services that deliver geographically diverse signal pathways, if possible, by:

a) Utilizing two independent managed facilities based voice network (MFVN) providers or;

b) Utilizing one managed facilities based voice network (MFVN) provider that provides contracted diverse signal pathways arranged so that the pathways are not likely to be affected by the same natural or man-made disasters or single point of failure.

RATIONALE FOR DECISION:

The intent of the additional paragraphs added to section 6 of UL 2050 is to have the monitoring stations equipped with redundancy. This will assure, if at any time the computer system and phone equipment were to fail there is a backup system that will automatically be in place to continue processing signals.

UL has found that the current edition of UL 2050 is silent on the redundancy and maintain operation if a single point were to fail. UL is introducing this concept to reduce and/or eliminate any point the computer system/automation system will be without signal processing.

UNDERWRITERS LABORATORIES INC. CERTIFICATION REQUIREMENT DECISION

This Certification Requirement Decision is prepared and published by Underwriters Laboratories Inc. (UL). It is normative for the applicable UL Product Certification Program(s); however, it is currently not part of the UL Standard(s) referenced below.

Product Category (CCN): CRZH & CRZM
Standard Number: UL 2050
Standard Title: National Industrial Security Systems
Edition Date: November 5, 2010
Edition Number: 5
Section / Paragraph Reference: 5.11, 6.3.5, 6.3.6, 6.3.7 – 16, and 6.3.17
Subject: Automation Systems

DECISION:

The additional paragraphs 5.11, 6.3.5, 6.3.6, 6.3.7 – 16, and 6.3.17 provide redundancy for the Government Contracting Monitoring Stations (GCMS) and National Industrial Monitoring Stations (NIMS) when using an automation system.

5.11 AUTOMATION SYSTEM – A computer system that consists of hardware and software components. These components include the alarm-monitoring software supplied by the automation system developer, the operating system, and programming languages, required to make the system operational. An automation system may be configured as a computer system that is directly connected to hardware based central-station receivers, internal software based receivers, or is connected to remote receivers located in central-stations other than the one where the automation system is located. It is used to automatically process change-of-status signals such as alarm, trouble, supervisory, disarming and arming (i. e. opening and closing), and similar signals that it receives from the central station receiving equipment. See the Standard for Central-Station Automation Systems, UL 1981.

6.3.5 A computer system is formed when the equipment includes power supplies, disk drives, processors, data storage devices, and similar components are interconnected to enable the alarm monitoring software to process signals.

6.3.6 Computer systems shall be designated, by the manufacturer with the following minimum specifications:

a) Designed for continuous use, 24 hours per day, 7 days per week;
b) Be specified by the manufacturer as a “high-availability” system;
c) Have no less than two cooling fans;
d) Have no less than two power supplies, each of which can supply power for the entire system; and
e) Have no less than two network connections, each of which can service all the system’s needs.

6.3.7 If an alarm monitoring automation system is used the following shall be met:

a) The central station shall maintain a dated diagram or printed description of the current configuration of the alarm monitoring automation system. The diagram or printed description shall be created when the automation system is installed and updated whenever there is a change to the system. The configuration shall be reviewed every 12 consecutive months and the records updated. The following should be included in the diagram or description as a minimum:
    1) All computers that form the automation system;
    2) All components that form a network for the automation system;
    3) All surge protective devices;
    4) All work stations by location;
    5) All network security measures, such as fire walls and the like;
    6) All network communication protocols;
    7) All communications channels that enter into the operating room; and

8) All WAN communications channels that penetrate the Central-station company facilities, that connect into the LAN.

6.3.8 If hardware virtualization techniques are used as part of a method to provide redundancy or failure tolerance:

a) The automation system shall be guaranteed sufficient resources within the system provisioning;

b) Additional partitions shall not have a higher priority than the automation system; and

c) The second or failover automation system shall reside on a separate whole hardware platform that has sufficient capacity to provide the same or greater alarm monitoring performance as the primary hardware.

6.3.9 An automation system shall be provided with the necessary spare parts, and personnel shall be trained to the necessary expertise to ensure that the system can be placed back in service within 24 hours of failure.

6.3.10 The system shall be configured so that redundant or failover components are engaged and actively processing signals at least once in every consecutive thirty day period.

6.3.11 Upon failure of the automation system's ability to process signals beyond the 90 seconds resumption time, the signal handling functions of the receivers connected to the automation system shall revert to their normal operation. These functions include displaying and recording all incoming signals and providing audible and visual indications of change-of-status signals.

6.3.12 Back-up copies of the automation system’s alarm system database shall be generated every 24 hours for restoring purposes. The most recent back-up copy shall be kept on-site in the event that problems develop with the alarm system data. At a minimum, back-up copies of the current alarm system database and alarm monitoring software shall be transferred to a secure off-site location two times in every seven day period.

6.3.13 A copy of the operating system shall be kept on-site and at an off-site location. The off-site location is not prohibited from being the software developer’s location, if a copy of the operating system can be delivered to the central station within 24 hours.

6.3.14 Access shall be provided to all back-up data records required and are maintained at an off-site location, this shall be provided at all times.

6.3.15 The back-up copy of the alarm monitoring software shall be stored at a secure off-site location in a manner that permits it to be readily available to central station personnel in the event it is needed for the restoration of the automation system after a failure.

6.3.16 Central station automation security measures over remote access shall comply with the following:

a) The following measures shall be taken to ensure appropriate secure access from sources outside of the central station.

1) Measure 1 – Physical security of facilities

i) Areas outside of the operating room, in a remote monitoring center, or in a redundant site housing equipment shall comply with physical security requirements.

ii) Areas housing terminals used to make temporary connections with the automation system by alarm service company managed locations shall be arranged in a manner that limits access and view to authorized employees of the location making the connection. When the area is not occupied, it shall be locked and protected by a Premises Extent 3 alarm system that is compliant with the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681.

The alarm system shall be monitored in the central station.

2) Measure 2 – Local Area Network (LAN) security measures, as outlined below, shall be applied.. These systems shall be maintained with the latest updates supplied by the manufacturer. .

3) Measure 3 – Wide Area Network (WAN) security

i) All communications shall employ the use of advanced encryption and other measures as documented, all of which shall be active at all times. These systems shall be maintained with the latest updates supplied by the manufacturer.

a1) Evidence of compliance from a Certificate of Authority (CA) for the validation of approved communication security functions shall be provided: or

a2) Evidence of compliance with the latest encryption National Institute of Standards & Technology (NIST) standard shall be provided.

b) Where the connection from the outside source is temporary, such as software vendor support, alarm service company, subscriber, and dealer, and/or from public safety answering points, it shall be made in compliance with the program access controls
described below:

1) Each individual authorized to access the system shall have a unique personal user name and password;

2) A user name shall consist of a minimum of six characters;

3) A password shall consist of a minimum of six alpha-numeric characters with at least one alpha and one numeric character;

4) After a maximum of five unsuccessful attempts to log on the username or password within 10 minutes, further attempts shall be automatically disabled;

5) The time, date, and identifying sign-on characteristic of the individual signing-on shall be recorded by the automation system at the time of signing-on;

6) The system shall prompt the user to change their security sign-on at intervals of three months or less.

7) A communication session shall be automatically terminated if it is idle for a maximum of 15 minutes; and

8) The ability to modify items within the automation system shall follow

RATIONALE FOR DECISION:

The intent of the additional paragraphs added to section 6 of UL 2050 is to have the monitoring stations equipped with redundancy. This will assure, if at any time the computer system were to fail there is a backup system that will automatically be in place to continue processing signals.

UL has found that the current edition of UL 2050 is silent on the redundancy and maintain operation if a single point were to fail. UL is introducing this concept to reduce and/or eliminate any point the computer system/automation system will be without signal processing.

General Services Administration

Contractor Procurement of GSA-Approved Security Containers

Procurement Steps

1. Authorization to store classified information

GSA Order OGP 4100.21 allows for contractors to procure through the GSA sources

(3) Fixed-price contractors (and subcontractors) purchasing security equipment.
Under 40 U.S.C. § 501, the Administrator has determined that fixed-price contractors and lower-tier subcontractors who are required to maintain custody of security classified records and information may purchase security equipment from GSA. Procedures for such acquisitions are set forth in 41 CFR 101-26.507.

Procurement Requirements

1. Must have requirement to store classified material and ensure contract authorizes storage. (DD 254 or equivalent)
2. Must have Activity Address Code, DoDAAC or GSA Account Code with contracting officers' authorization OR can get own eDoDAAD.
3. Must be able to pay (GPC, AAC/DoDAAC, MIPR, VCSS, pay.gov, credit/debit card, Paypal/Amazon Pay, Bank Account)
4. Order Security Equipment offline or online thru GSA

Step 1: Requirement and Authorization

Must have requirement to store classified material and ensure contract authorizes storage. (DD 254 or equivalent)

Work with your Contracting Officer to insert the appropriate clause allowing use of Government sources of supply if not already included. (Contract Clause 252.251-7000 ORDERING FROM GOVERNMENT SUPPLY SOURCES (NOV 2004))

Step 2: Activity Address Code, DoDAAC, eDoDAAD

If you already have an Activity Address Code, DoDAAC or eDoDAAD, please skip to step 3 (page 5)

- Must have Activity Address Code, DoDAAC or GSA Account Code with contracting officers' authorization OR can get own eDoDAAD.
- Link to get eDoDAAD: https://www.dla.mil/HQ/InformationOperations/DLMS/DLMSPrograms/DoDAAD/

Step 3: Payment

Forms of payment include:

A. Payment forms accepted:
   - Government Purchase Card
   - AAC/DoDAAAC
   - Bank Account
   - Credit /Debit card
   - Paypal /Amazon Pay

B. Use Vendor Customer Support Service (VCSS) account to see bills

C. Use pay.gov to pay bills

If you have concerns/issues with payments such as paypal, bank card, etc…, contact your POC for the appropriate payment method at your activity.

Step 4: Ordering Security Equipment

Order Security Equipment online or offline thru GSA See next slides for assistance

- If further explanation is required, you can obtain detailed procedures on GSA's website:
- https://www.gsa.gov/buying-selling/purchasing-programs/requisition-programs/gsa-global-supply/nsns-and-product-lines/security-containers/ordering-procedures-for-security-containers
- For Assistance with completing requisitions and identifying or validating DoDAAC you can contact Sheila.Patterson@gsa.gov
- For Assistance with item identification/clarification (NSN) and Order Status contact Security Container General Mailbox securitycontainers@gsa.gov or Martin.Cieszlak@gsa.gov

Step 4: Ordering Security Equipment - **Online**

Online – to order online you must have the following available:

1. .mil or .gov email address
2. Activity Address Code
3. Form of Payment and/or Codes
4. National Stock Number for Security Container that you want to order – See page 13 for how to find NSN's
5. To place order go to www.gsaglobalsupply.gsa.gov or www.gsaadvantage.gov

Step 4: Ordering Security Equipment - **Offline**

Offline – order offline by FEDSTRIP or MILSTRIP

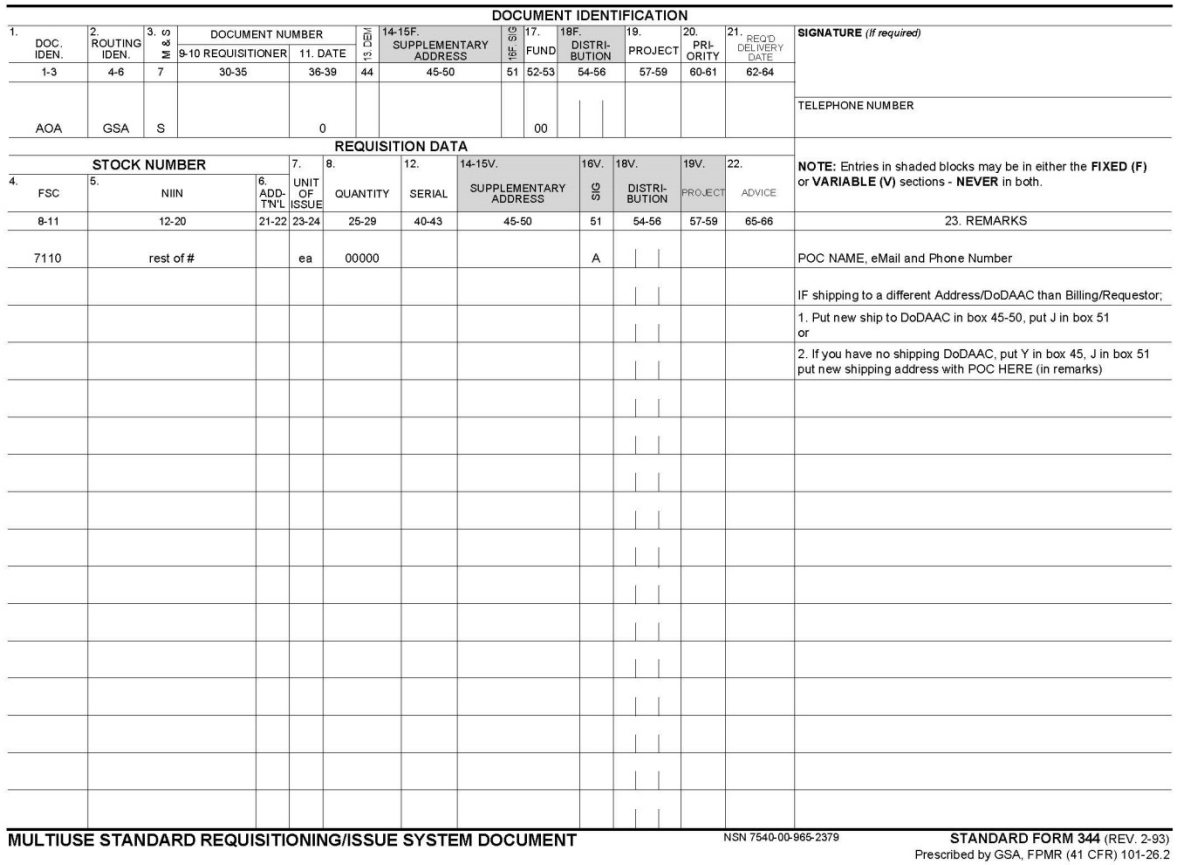
- Orders can be placed “offline” through DD Form 1348 (MILSTRIP) or Standard Form 344 (FEDSTRIP).
- Submit completed forms to GSA's Requisitioning Processing & Customer Center at: rpc@gsa.gov and copy the Security Container Team at: securitycontainers@gsa.gov.

See following pages for assistance with forms.

How to Fill out Offline Forms

FEDSTRIP – Standard From 344

Link to FEDSTRIP form that you can fill out: https://www.gsa.gov/cdnstatic/SF_344_fillable.pdf



DOCUMENT IDENTIFICATION

1. DOC. IDEN.	2. ROUTING IDEN.	3. M	DOCUMENT NUMBER 9-10 REQUISITIONER	11. DATE	13. DEM	14-15F. SUPPLEMENTARY ADDRESS	16F. SIG	17. FUND	18F. DISTRI-BUTION	19. PROJECT	20. PRI-ORITY	21. REQ'D DELIVERY DATE	SIGNATURE *(If required)*
1-3	4-6	7	30-35	36-39	44	45-50	51	52-53	54-56	57-59	60-61	62-64	
AOA	GSA	S		0				00					TELEPHONE NUMBER

REQUISITION DATA

STOCK NUMBER 4. FSC	5. NIIN	6. ADD-TN'L	7. UNIT OF ISSUE	8. QUANTITY	12. SERIAL	14-15V. SUPPLEMENTARY ADDRESS	16V. SIG	18V. DISTRI-BUTION	19V. PROJECT	22. ADVICE	NOTE: Entries in shaded blocks may be in either the **FIXED (F)** or **VARIABLE (V)** sections - **NEVER** in both.
8-11	12-20	21-22	23-24	25-29	40-43	45-50	51	54-56	57-59	65-66	23. REMARKS
7110	rest of #		ea	00000			A				POC NAME, eMail and Phone Number
											IF shipping to a different Address/DoDAAC than Billing/Requestor;
											1. Put new ship to DoDAAC in box 45-50, put J in box 51 or
											2. If you have no shipping DoDAAC, put Y in box 45, J in box 51 put new shipping address with POC HERE (in remarks)

MULTIUSE STANDARD REQUISITIONING/ISSUE SYSTEM DOCUMENT NSN 7540-00-965-2379 **STANDARD FORM 344** (REV. 2-93) Prescribed by GSA, FPMR (41 CFR) 101-26.2

Specifics for ordering containers using FEDSTRIP (344)

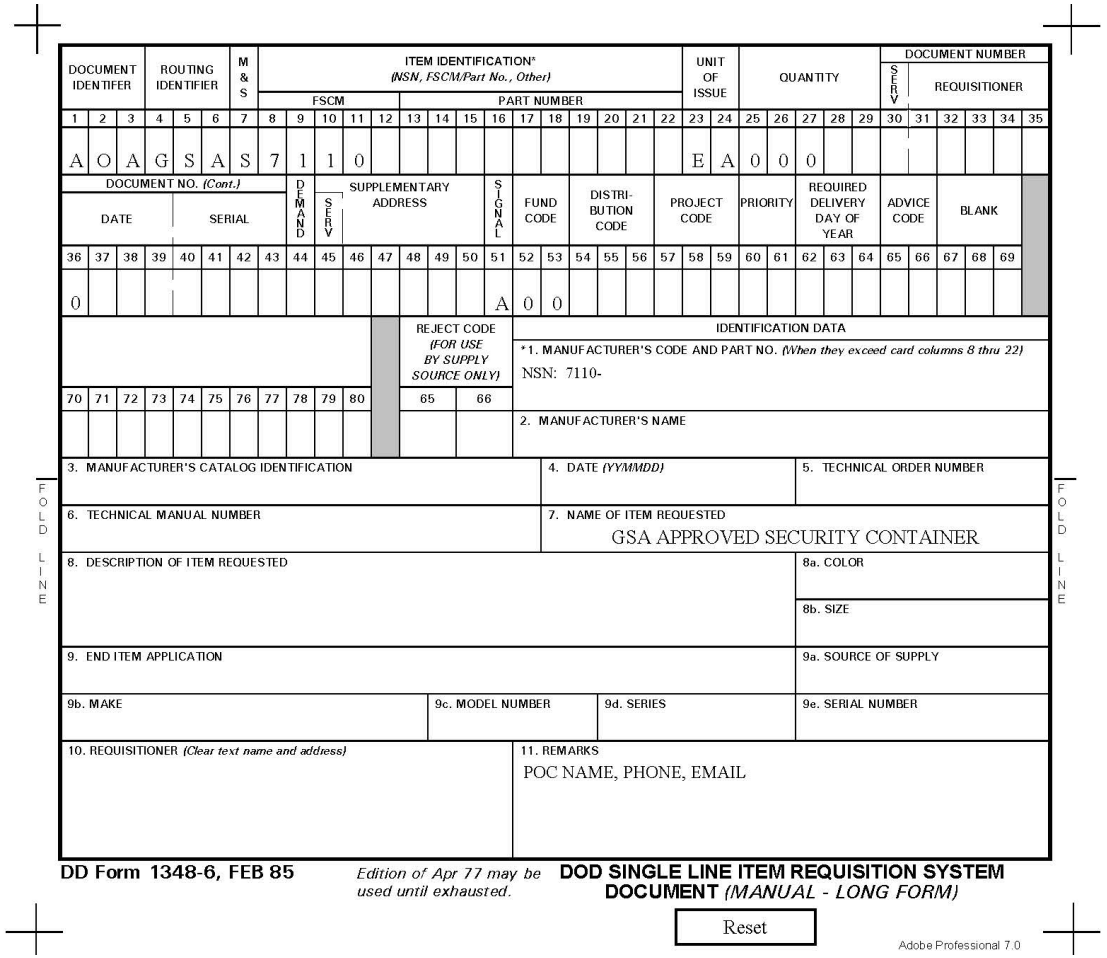
- On the previous slide you will see that there are some fields that are already filled out.
- These are the fields that will not change:
- Boxes
- 1-3: AOA
- 4-6: GSA
- 7: S
- 8-11: 7110
- 23-24: EA
- 51: A
- 52-53: 00

- Fields that Change:
- 12-20 rest of National Stock Number (9 digits)
- 25-29 Quantity
- 30-35 Billing DoDAAC
- 36-39 Julian Date, for 2020 will start with 0 then 3 digits for day of year
- 45-50 Ship To DoDAAC (if different than Billing) see form for codes to place into other boxes if this is your requirement
- 60-61 06 to 13
- Block 23 Remarks – should have your POC's Name, Phone and E:Mail, can also put in alternate delivery address in this block

How to Fill out Offline Forms

MILSTRIP – DD From 1348

Link to MILSTRIP form that you can fill out: https://www.gsa.gov/cdnstatic/DD1348-6_FillableForm.pdf



DOCUMENT IDENTIFER	ROUTING IDENTIFIER	M & S	ITEM IDENTIFICATION* (NSN, FSCM/Part No., Other) FSCM	PART NUMBER	UNIT OF ISSUE	QUANTITY	DOCUMENT NUMBER SERV	REQUISITIONER
1 2 3	4 5 6	7	8 9 10 11 12	13 14 15 16 17 18 19 20 21 22	23 24	25 26 27 28 29	30	31 32 33 34 35
A O A	G S A	S	7 1 1 0		E A	0 0 0		

DOCUMENT NO. (Cont.) DATE	SERIAL	DEMAND	SUPPLEMENTARY ADDRESS SERV		SIGNAL	FUND CODE	DISTRI-BUTION CODE	PROJECT CODE	PRIORITY	REQUIRED DELIVERY DAY OF YEAR	ADVICE CODE	BLANK
36 37 38 39 40 41	42 43	44	45	46 47 48 49 50	51	52 53	54 55 56	57 58 59	60 61	62 63 64	65 66	67 68 69
0					A	0 0						

REJECT CODE (FOR USE BY SUPPLY SOURCE ONLY)	IDENTIFICATION DATA
70 71 72 73 74 75 76 77 78 79 80 65 66	*1. MANUFACTURER'S CODE AND PART NO. (When they exceed card columns 8 thru 22) NSN: 7110-
	2. MANUFACTURER'S NAME

3. MANUFACTURER'S CATALOG IDENTIFICATION	4. DATE (YYMMDD)	5. TECHNICAL ORDER NUMBER
6. TECHNICAL MANUAL NUMBER	7. NAME OF ITEM REQUESTED GSA APPROVED SECURITY CONTAINER	
8. DESCRIPTION OF ITEM REQUESTED		8a. COLOR
		8b. SIZE
9. END ITEM APPLICATION		9a. SOURCE OF SUPPLY
9b. MAKE	9c. MODEL NUMBER / 9d. SERIES	9e. SERIAL NUMBER
10. REQUISITIONER (Clear text name and address)	11. REMARKS POC NAME, PHONE, EMAIL	

FOLD LINE FOLD LINE

DD Form 1348-6, FEB 85 — Edition of Apr 77 may be used until exhausted. — DOD SINGLE LINE ITEM REQUISITION SYSTEM DOCUMENT (MANUAL - LONG FORM)

Reset

Adobe Professional 7.0

Specifics for ordering GSA Approved containers using MILSTRIP (1348)

- On the previous slide you will see that there are some fields that are already filled out.
- These are the fields that will not change:
- Boxes
- 1-3: AOA
- 4-6: GSA
- 7: S
- 8-11: 7110
- 23-24: EA
- 51: A
- 52-53: 00

- Fields that Change:
- 12-20 rest of National Stock Number (9 digits)
- 25-29 Quantity
- 30-35 Billing DoDAAC
- 36-39 Julian Date, for 2020 will start with 0 then 3 digits for day of year
- 45-50 Ship To DoDAAC (if different than Billing) see form for codes to place into
- other boxes if this is your requirement
- 60-61 06 to 13
- Block 11 Remarks – should have your POC's Name, Phone and e:Mail, can also put in alternate delivery address in this block

Where to Find National Stock Numbers

NOTE: Some sources have pictures that do not correspond with the stock number listed. Read description of what you are purchasing/looking for when obtaining number.

- https://cmls.gsa.gov/CMLSPubCategory?searchKey=CA-0025721 – website for Global Supply Security Container Catalog
- https://www.gsa.gov/buying-selling/purchasing-programs/requisition-programs/gsa-global-supply/nsns-and-product-lines/security-containers/types-of-security-containers – website for Security Container Descriptions, Uses and NSN's, with each container type in separate .pdf.

Additional Resources

Step-by-step Contractor Purchasing Guide:

https://www.gsa.gov/cdnstatic/General_Supplies__Services/Non-Government_Ordering_Process_for_Security_Equipment_%282019%29_508.pdf

DoD Lock Program – One stop tool for technical information and updates to the security program

https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html

DLA FAQ

https://www.dla.mil/HQ/InformationOperations/Defense-Logistics-Management-Standards/faq/

GSA Supply Catalog 2020

https://cmls.gsa.gov/CMLSPubCategory?searchKey=CA-0025721


GENERAL SERVICES
ADMINISTRATION

GSA APPROVED SECURITY EQUIPMENT - PURCHASING GUIDE

Government agency customers please refer to your agency POC for help with GSA ordering

This letter has been prepared to give guidance to non-government entities under contract with the Federal Government ("contractors") on the correct ordering procedure for GSA Approved security containers and vault doors ("security equipment"). The following information can help direct you to useful resources, but will not do the work for you. You are responsible for working diligently with a contracting officer and taking action that is appropriate for your situation.

Summary:

1. Ensure your contract authorizes you to store classified material
2. Work with a contracting officer to set up an Activity Address Code
3. Order through FEDSTRIP/MILSTRIP or GSA Global Supply/*Advantage!*
4. Appendix A-E:
    A. 41 CFR § 101-26.507 – Security equipment
    B. GSA Order OGP 4800.2I – Eligibility to Use GSA Sources of Supply and Services
    C. DLM 4000.25 Volume 6 Chapter 2.4.1.2 – DoD Contractor DoDAACs
    D. FAR Part 51 – Use of Government Supply Sources by Contractors (Condensed)
    E. PGI 251.102 – Authorization to use Government supply sources

What is happening to the "exemption process"?

After October 1, exemptions to bypass Global Supply will no longer be given to federal contractors. ISOO Notice 2014-02 prescribes that security equipment "must now be procured through GSA Global Supply." In order to ensure the continued availability of security equipment, the exemption process was set up as a temporary means of procuring security equipment while contractors amended their contracts to comply with the ISOO Notice. As detailed in IACSE Letter "End of the Exemption Process" (May 30, 2019), sufficient time has passed since the ISOO Notice was issued for such changes to happen.

Why must security equipment be ordered through GSA?

GSA Approved security equipment is restricted for use only by the US Government and approved federal contractors. Using GSA ensures that all purchases are in compliance with Federal Regulations (**Appendix A,** CFR) and improves GSA's ability to ensure quality customer service. Moreover, it ensures that any security equipment you purchase meets federal testing requirements and specifications.

1. AUTHORIZATION TO STORE CLASSIFIED MATERIAL:

GSA Order OGP 4800.2I specifies that contractors who are required to maintain custody of classified information are permitted to purchase security equipment through GSA sources (**Appendix B**, GSA

Order). Your contract must include a DD Form 254 (or equivalent), which provides classification requirements and guidance to the contractor.

2. ACTIVITY ADDRESS CODE:

What is an Activity Address Code?

An Activity Address Code (AAC, DoDAAC for DoD customers, and sometimes referred to as a GSA Account Code) is a six digit code "that uniquely identifies a unit, activity, or organization that has the authority to requisition, contract for, receive, have custody of, issue, or ship government owned assets, or fund/pay bills for materials and/or services" (DLA FAQ 19). The codes are used when ordering supplies from the government supply system with FEDSTRIP, MILSTRIP, or DLMS. The AAC also stores payment and shipment information. Orders for GSA-supplied items (like security containers) must be placed with an AAC or government purchase card.

Who can have an AAC?

If your contract authorizes you to store classified material, you can apply for an

AAC. **How do I get an AAC?**

Work with a contracting officer who is familiar with your contract to take appropriate steps.

DoD contractors can request a DoDAAC through the Contractor DoDAAC request module in the Procurement Integrated Enterprise Environment (PIEE) (**Appendix C,** DLM). That request will be validated against the relevant contract.

See **Appendix D**, FAR, for details of steps and information required to manually apply for an AAC. A contracting officer can fill out form PGI 251.102 (**Appendix E**), which follows along with FAR 51.102 to organize the required information.

3. ORDERING SECURITY EQUIPMENT:

Once you receive an AAC, see detailed ordering procedures here:
https://www.gsa.gov/buying-selling/purchasing-programs/requisition-programs/gsa-global-supply/nsns-and-product lines/security-containers/ordering-procedures-for-security-containers

These procedures are summarized below.

Ordering through GSA Global Supply

If you have an account or can set one up, ordering through GSA Global Supply or Advantage is the easiest option (Requires and approved email domain such as .gov or .mil). You may place your order on-line via GSA Global Supply at: www.gsaglobalsupply.gsa.gov or GSA Advantage at: https://www.gsaadvantage.gov. Both sites function 24/7, enabling users to place orders from anywhere in the world, and offer electronic equivalents of traditional requisition forms DD 1348 or SF 344.

Payment: GSA Global Supply accepts your GPC or direct billing through your AAC or DoDAAC. Shipping/Freight Charges: GSA prices are FOB origin, Freight - prepay and add.

Ordering with FEDSTRIP/MILSTRIP

Orders can be placed “offline” through DD Form 1348 (MILSTRIP) or Standard Form 344 (FDSTRIP). Copies of these forms are at the ordering procedures link above.

Please submit your completed forms to GSA's Requisitioning Processing & Customer Center at: rpc@gsa.gov and copy the Security Container Team at: securitycontainers@gsa.gov.

Instructions for MILSTRIP:
https://www.gsa.gov/cdnstatic/MILSTRIP_Instructions.pdf

Instructions for FEDSTRIP:
https://www.gsaadvantage.gov/images/muffin/fedstrip_guide_2006.pdf

Special Requests

If you are requesting a specific manufacturer, expedited delivery or require a lift gate and/or inside delivery, please e-mail the Security Container general mailbox at: securitycontainers@gsa.gov. In your email reference your requisition number and state your special request. If you place your order on-line via GSA Advantage or GSA Global Supply, please forward a copy of your confirmation e-mail, to include your special request information.

Additional Information:

DoD Lock Program – One stop tool for technical information and updates to the security program
https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html

DLA FAQ
https://www.dla.mil/HQ/InformationOperations/Defense-Logistics-Management-Standards/faq/

GSA Supply Catalog 2020 (see pg. 260-267 for containers)
https://cmls.gsa.gov/servlet/servlet.FileDownload?retURL=%2Fapex%2FCMLSPubCategory%3FsearchKey%3D05-19-00382&file=00Pt000000Fe72HEAR

4. APPENDIX:

Appendix A. 41 CFR § 101-26.507 – **Security equipment**

Federal agencies and other activities authorized to purchase security equipment through GSA sources shall do so in accordance with the provisions of this § 101-26.507. Under section 201 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 481), the Administrator of GSA has determined that fixed-price contractors and lower tier subcontractors who are required to protect and maintain custody of security classified records and information may purchase security equipment from GSA sources. Delivery orders for security equipment submitted by such contractors and lower tier subcontractors shall contain a statement that the security equipment is needed for housing Government security classified information and that the purchase of such equipment is required to comply with the security provision of a Government contract. In the event of any inconsistency between the terms and conditions of the delivery order and those of the Federal Supply Schedule contract, the latter shall govern. Security equipment shall be used as prescribed by the cognizant security office.
[60 FR 19675, Apr. 20, 1995]

Appendix B. GSA Order OGP 4800.2I – **Eligibility to Use GSA Sources of Supply and Services**

7. Eligible activities.
Organizations are eligible to use GSA sources of supply and services pursuant to 40 U.S.C. §§ 501 - 502 or other statutory authority; however, some organizations may be eligible to use only specific GSA sources of supply or services. In addition, although an organization may be eligible to use GSA sources of supply, particular sources may not be accessible due to limits of supply sources or geographical constraints. For example, in the case of GSA Fleet, it may not be practical for GSA to make certain sources of supply available. In addition, the terms of a specific contract may not permit participation by otherwise eligible organizations. Other organizations authorized under the authority of 40 U.S.C. §§ 501 - 502. GSA has determined that certain organizations, other than those described above, are eligible to use its sources of supply and services under the authority provided to the Administrator by 40 U.S.C. §§ 501 - 502.

d. Other organizations authorized under the authority of 40 U.S.C. §§ 501 - 502.
GSA has determined that certain organizations, other than those described above, are eligible to use its sources of supply and services under the authority provided to the Administrator by 40 U.S.C. §§ 501 - 502.

(3) Fixed-price contractors (and subcontractors) purchasing **security equipment.**
Under 40 U.S.C. § 501, the Administrator has determined that fixed-price contractors and lower-tier subcontractors who are required to maintain custody of security classified records and information may purchase security equipment from GSA. Procedures for such acquisitions are set forth in 41 CFR 101-26.507.

Appendix C. DLM 4000.25 Volume 6 Chapter 2 – **DoD Contractor DoDAACs**

2.4.1.2: DoD contractors ***(CTR)*** will only be assigned DoDAACs if they have a contract with DoD that authorizes access to DoD supply system materiel or to provide services such as maintenance/repair that require a shipping address. Contractor DoDAACs ***may be requested by anyone related to the contract/program through the Contractor DoDAAC request module in the Procurement Integrated Enterprise Environment (PIEE). The requestor will indicate whether the DoDAAC should have requisitioning authority or just be a shipping location. Requisitioning DoDAAC requests will be validated against the contract to confirm the contract allows such authority. In addition to appropriate address information, requestors will ensure the following contract information data elements are entered for every contractor DoDAAC. All are mandatory fields except for Order Number and Contract Period of Performance End date, which are situationally dependent*** (for all non-contractor DoDAACs, these fields are disabled).

Appendix D. FAR Part 51 – **Use of Government Supply Sources by Contractors** (Condensed)

51.101 Policy.

(a) If it is in the Government's interest, and if supplies or services required in the performance of a Government contract are available from Government supply sources, contracting officers may authorize contractors to use these sources in performing

(1) Government cost-reimbursement contracts;
(2) Other types of negotiated contracts when the agency determines that a substantial dollar portion of the contractor's contracts are of a Government cost-reimbursement nature; or

(b) Contractors with fixed-price Government contracts that require protection of security classified information may acquire security equipment through GSA sources (see 41 CFR 101-26.507).

51.102 Authorization to use Government supply sources.

(a) Before issuing an authorization to a contractor to use Government supply sources in accordance with 51.101(a) or (b), the contracting officer shall place in the contract file a written finding supporting issuance of the authorization. A written finding is not required when authorizing use of Government supply sources in accordance with 51.101(c). Except for findings under 51.101(a)(3), the determination shall be based on, but not limited to, considerations of the following factors:

(1) The administrative cost of placing orders with Government supply sources and the program impact of delay factors, if any.
(2) The lower cost of items available through Government supply sources.
(3) Suitability of items available through Government supply sources.
(4) Delivery factors such as cost and time.
(5) Recommendations of the contractor.

(b) Authorizations to subcontractors shall be issued through, and with the approval of, the contractor.

(c) Upon deciding to authorize a contractor to use Government supply sources, the contracting officer shall request, in writing, as applicable-

(1) A FEDSTRIP activity address code, through the agency's central contact point for matters involving activity address codes, from the General Services Administration (GSA) FXS Washington, DC 20406;
(2) A MILSTRIP activity address code from the appropriate Department of Defense (DoD) service point listed in Section1 of the Introduction to the DoD Activity Address Directory;

(d) Each request made under paragraph (c) of this section shall contain-

(1) The complete address(es) to which the contractor's mail, freight, and billing documents are to be directed; (2) A copy of the contracting officer's letter of authorization to the contractor;
(3) The prime contract number(s); and
(4) The effective date and duration of each contract.

(e) In each authorization to the contractor, the contracting officer-

(1) Shall cite the contract number(s) involved;
(2) Shall, when practicable, limit the period of the authorization;

(3) Shall specify, as appropriate, that-

(i) When requisitioning from GSA or DoD, the contractor shall use FEDSTRIP or MILSTRIP, as appropriate, and include the activity address code assigned by GSA or DoD;

51.103 Ordering from Government supply sources.

(a) Contractors placing orders under Federal Supply Schedules shall follow the terms of the applicable schedule and authorization and include with each order-

(1) A copy of the authorization (unless a copy was previously furnished to the Federal Supply Schedule contractor); and
(2) The following statement: This order is placed under written authorization from _____ dated _____. In the event of any inconsistency between the terms and conditions of this order and those of your Federal Supply Schedule contract, the latter will govern.

(b) Contractors placing orders for Government stock shall-

(1) Comply with the requirements of the contracting officer's authorization, using FEDSTRIP or MILSTRIP procedures, as appropriate;
(2) Use only the Government activity address code obtained by the contracting officer in accordance with 51.102(e) along with the contractor's assigned access code, when ordering from GSA Customer Supply Centers. (3) Order only those items required in the performance of their contracts.

51.104 Furnishing assistance to contractors.

After receiving an activity address code, the contracting officer will notify the appropriate GSA regional office or military activity, which will contact the contractor and-

(a) Provide initial copies of ordering information and instructions; and

(b) When necessary, assist the contractor in preparing and submitting, as appropriate-

(1) The initial FEDSTRIP or MILSTRIP requisitions, the Optional Form 347, or the agency-approved forms; (2) A completed GSA Form 457, FSS Publications Mailing List Application, so that the contractor will automatically receive current copies of required publications; or
(3) A completed GSA Form 3525, Application for Customer Supply Center Services and (Address Change).

Appendix E. PGI 251.102 **– Authorization to use Government supply sources.**

Use a format substantially the same as the following when authorizing contractor use of Government Supply Sources. Specify the terms of the purchase, including contractor acceptance of any Government materiel, payment terms, and the addresses required by paragraph (e) of the clause at 252.251-7000, ordering from Government Supply Sources.

AUTHORIZATION TO PURCHASE FROM GOVERNMENT SUPPLY SOURCES

(SAMPLE FORMAT)

SUBJECT: Authorization to Purchase from Government Supply Sources

_____(Contractor's Name)

_____(Contractor's Address)

_____(CAGE Code)

1. You are hereby authorized to use Government sources in performing Contract No. _____ for *[insert the requiring activity's DoD Activity Address Code (DoDAAC)]*, as follows: *[Insert applicable purchasing authority given to the contractor.]*

2.a. Purchase Orders Under Federal Supply Schedules or Personal Property Rehabilitation Price Schedules. Place orders in accordance with the terms and conditions of the attached Schedule(s) and this authorization. Attach a copy of this authorization to the order (unless a copy was previously furnished to the Federal Supply Schedule or Personal Property Rehabilitation Price Schedule contractor). Insert the following statement in the order:

This order is placed under written authorization from _____ dated _____ (*_____). In the event of any inconsistency between the terms and conditions of this order and those of the Federal Supply Schedule or Personal Property Rehabilitation Price Schedule contract, the latter will govern.

b. Requisitioning from the General Services Administration (GSA) or the Department of Defense (DoD). Place orders in accordance with this authorization and, as appropriate, the following:

(1) Federal Standard Requisitioning and Issue Procedures (FEDSTRIP) (GSA FEDSTRIP Operating Guide: FPMR 101-26.2 (41 CFR 101-26.2)). Copies are available from the Superintendent of Documents, Government Printing Office, Washington, DC 20402; telephone (202) 512-1800; facsimile (202) 512-2250.

(2) Military Standard Requisitioning and Issue Procedures (MILSTRIP) (DoD 4000.25-1-M). Copies are available from the Defense Logistics Agency, Administrative Support Center East, ATTN: ASCE-WS, 14 Dedication Drive, Suite 3, POD 43, New Cumberland, PA 17070-5011; telephone 1-888-DLA-PUBS(352-7827), or (717) 770- 6034; facsimile (717) 770-4817.

c. Enterprise Software Initiative. Place orders in accordance with the terms and conditions of the attached Enterprise Software Agreement(s), or instructions for obtaining commercial software or software maintenance from Enterprise Software Initiative inventories, and this authorization. Attach a copy of this authorization to the order (unless a copy was previously furnished to the Enterprise Software Agreement contractor). Insert the following

statement in the order:

This order is placed under written authorization from _____ dated_____ (*_____). In the event of any inconsistency between the terms and conditions of this order, and those of the Enterprise Software Agreement, the latter will govern.

3. *[Insert other provisions as necessary.]*

4. This authority is not transferable or assignable.

5. The DoD Activity Address Directory (DoDAAD) (DLM 4000.25, Volume 6, Chapter 2) Activity Address Code** to which this Authorization applies is _____.

6. This Authorization expires _____.

_____

(Contracting Officer)

* Insert "a copy of which is attached," "a copy of which you have on file," or other suitable language, as appropriate.

** The requiring activity assumes responsibility for monitoring and controlling all activity address codes used in the letters of authority.

PGI 251.102-70 Contracting office responsibilities.

(a) The DoD Activity Address Code (DoDAAC) assigned in accordance with paragraph 5 of the authorization format in PGI 251.102 (DFARS/PGI view) shall be assigned to the contractor for authorization to use Government supply sources only for the contract number cited in paragraph 1 of the authorization format.

(b) The authorization to use Government sources of supply is unique to each contract and shall not be transferred or assigned to any other contractor or contract. Therefore, the same DoDAAC shall not be assigned to any other contract number during the period of performance for the contract. After 24 months has lapsed beyond contract closeout, the DoDAAC may be reused for another contract.

NISA WG Update
April 2022 NISPPAC Public Meeting

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

NISP Authorization Office (NAO)
April 27, 2022

NISP AUTHORIZATION OFFICE

Discussion Topics

- NAO Workforce Updates
- NISP eMASS Enhancements
- NISP Connection Process Guide (CPG) Update
- NAO – What is Next?

NISP AUTHORIZATION OFFICE

- NISP AO Leadership
  - NAO: David Scott

- Regional Leadership
  - Mid-Atlantic Region AO: Ezekiel Marshall
  - Eastern Region AO: Alexander Hubert
  - Central Region AO: William Vaughn
  - Western Region AO: Stacey Omo

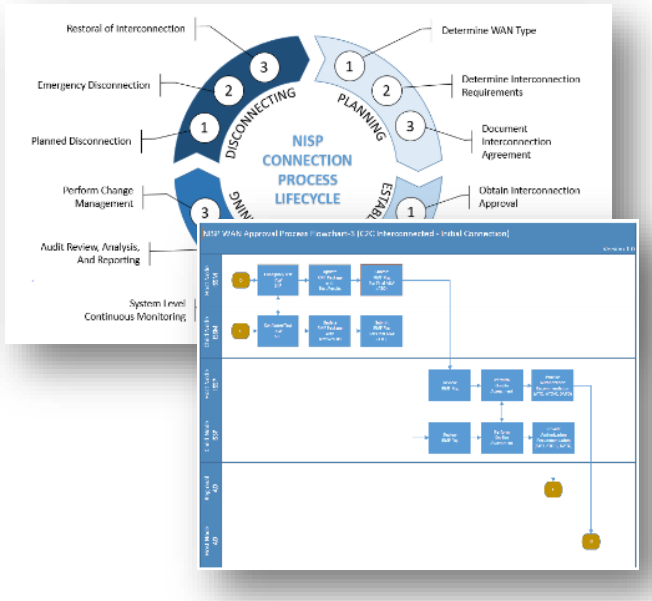
NISP AUTHORIZATION OFFICE

NISP eMASS Package Approval Chain Workflow Enhancements

- On January 6, 2022, the Package Approval Chain (PAC) workflows were enhanced in order to maximize Industry's visibility into the Assessment and Authorization (A&A) process. When submitting System Security Plans (SSP), Industry will submit security controls within the Control Approval Chain (CAC) and also initiate the applicable PAC workflow.
- By initiating the PAC workflows, Industry will be able to accurately track all stages of the A&A process and utilize key functions of eMASS (e.g., Workflow Tracking, Workload Tasks, Collaboration Board, etc.).
- In order to ensure that Industry understands the SSP submission process, the NAO released the New NISP eMASS SSP Instructions. The instructions are available on the NISP eMASS [HELP] Page. Also, the NAO will soon be releasing the NISP eMASS SSP Guidance. The guide will provide additional clarification.
- For NISP eMASS related questions or concerns, please contact the DCSA NAO eMASS Team (dcsa.quantico.dcsa.mbx.emass@mail.mil).

NISP AUTHORIZATION OFFICE

- NISP CPG Goal:
  - Provides guidelines for interconnecting systems processing classified information within the NISP
  - Easy to read guide format for government and industry stakeholders
    - Step by Step process, templates & enhanced guidance
    - RMF control mappings
  - Creates efficiencies for all NISP stakeholders & enhances security
  - New concepts such as:
    - Ports, Protocols, & Services Management (PPSM)
    - Corresponding Risk Levels with security posture guidance



- NISP CPG Status
  - Completed coordination with the NISA Working Group participants March 2022
  - Formal Coordination to begin
  - Publication date – TBD

NISP AUTHORIZATION OFFICE

NAO What's Next?

- eMASS
  - Job Aids & additional guidance.
- DAAPM 3.0
  - Provide enhanced guidance & clarity for industry.
  - Process improvements, identifying and addressing any gaps.
- Command Cyber Readiness Inspections (CCRI).
- Continued collaboration with NISP stakeholders.

End of Briefing

For questions or concerns, Cleared Industry should consult with their local ISSP.

eMASS/RMF Resources are located at:

https://www.dcsa.mil/mc/ctp/tools/

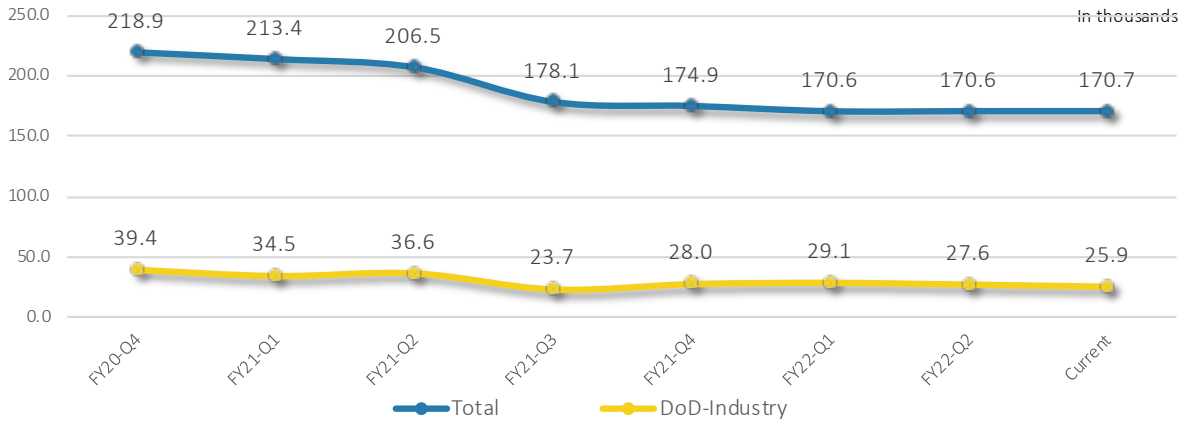
NISP eMASS Mailbox:

dcsa.quantico.dcsa.mbx.emass@mail.mil

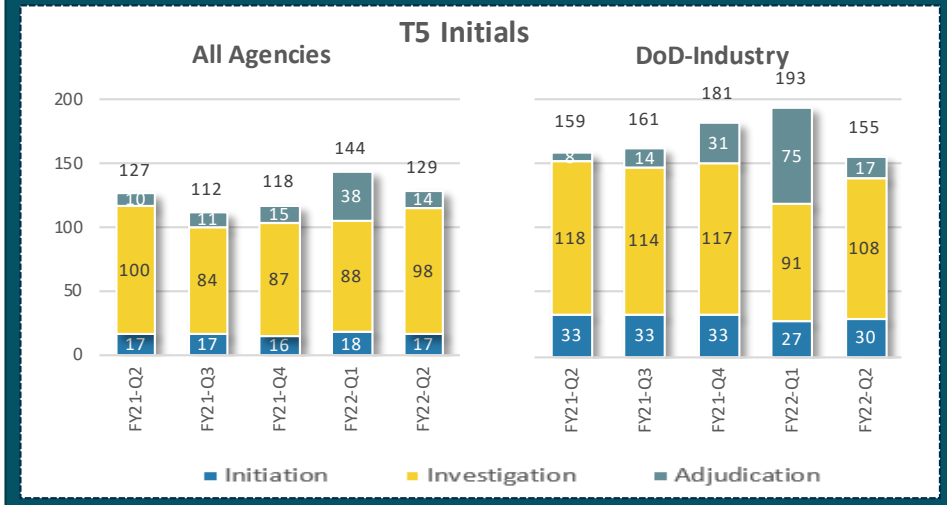
DCSA INVESTIGATION INVENTORY & TIMELINESS | *Industry*

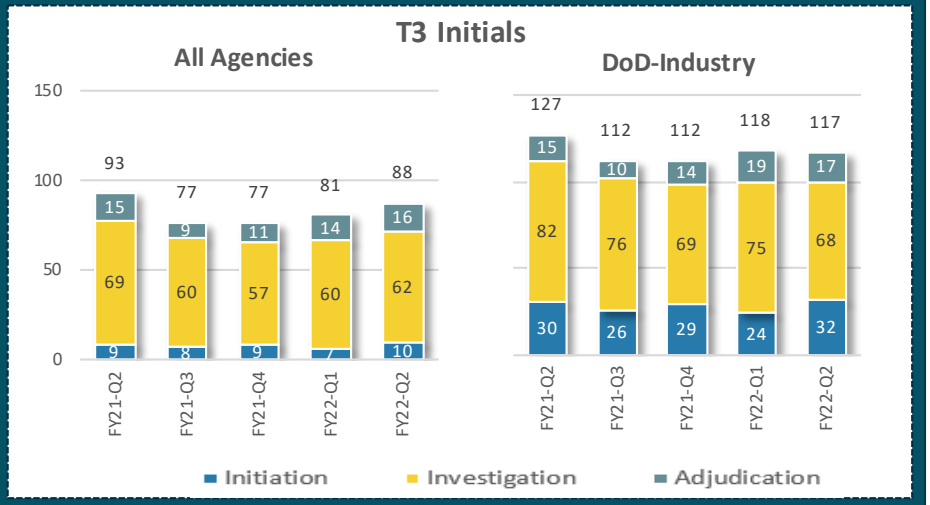
INVESTIGATION

CURRENT INVENTORY	
All DCSA Customers	170.7K
Industry Only	25.9K

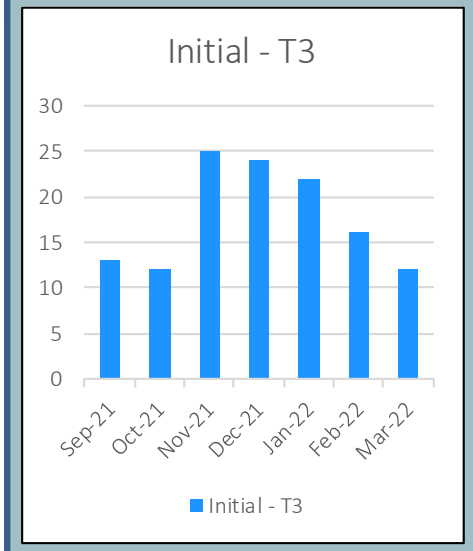


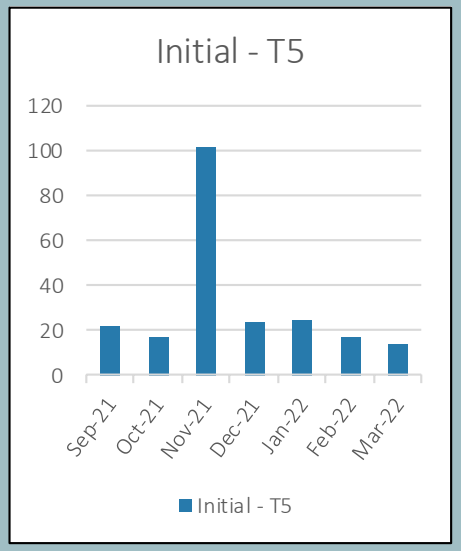
END-TO-END TIMELINESS (Fastest 90% of adjudicated investigations in days)

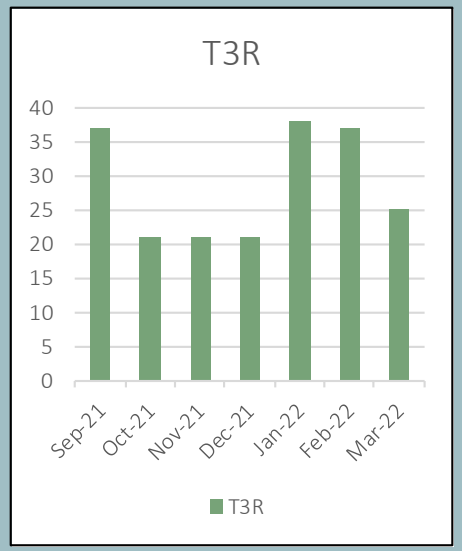


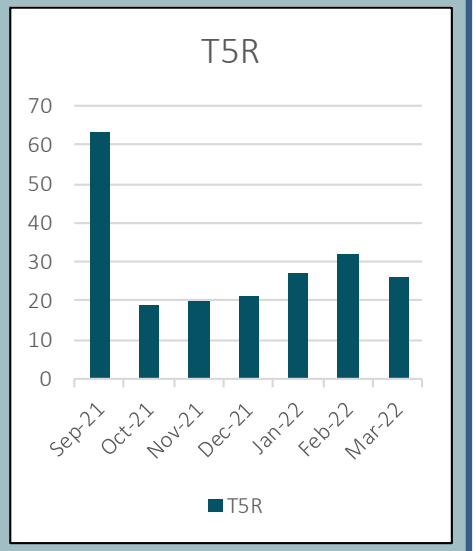


Adjudications Timeliness For Industry FY22-YTD









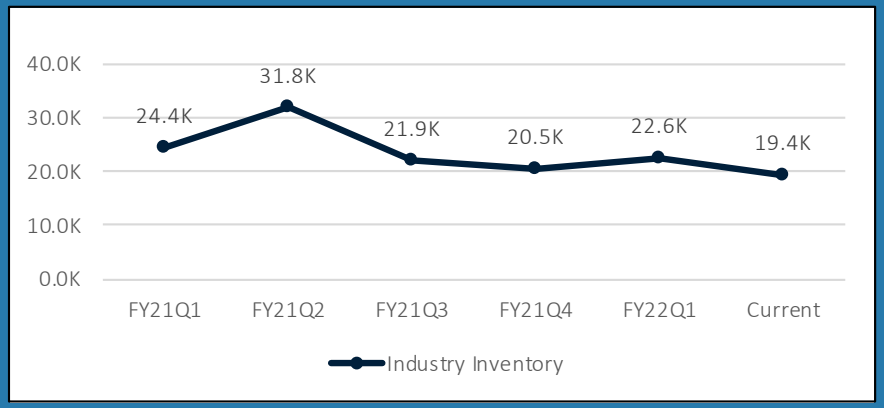
Industry Quarterly Timeliness

Industry	Secret	Top Secret	Secret Reinvestigation	Top Secret Reinvestigation
FY21Q1	14	13	31	30
FY21Q2	20	8	49	66
FY21Q3	11	13	33	28
FY21Q4	13	30	40	33
FY22Q1	19	75	19	20
FY22Q2	17	17	33	28

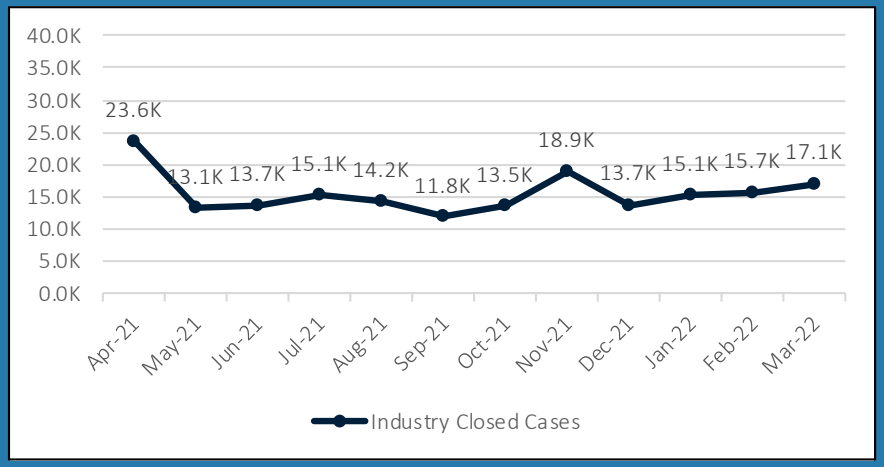
Report Date: 4/1/2022
OPR: DCSA ADJ Metrics Team

Adjudications Inventory For Industry FY22-YTD

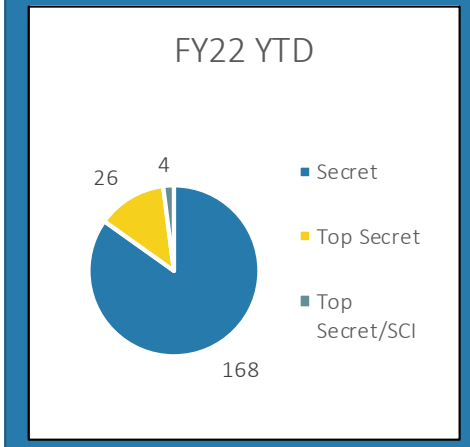
INDUSTRY CURRENT INVENTORY	
Industry	19.4K

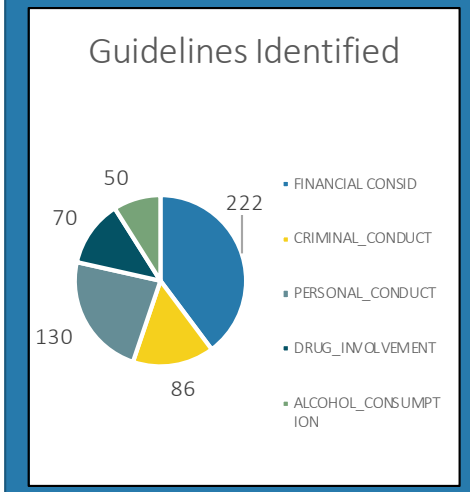


Industry Closed Cases	
FY21Q1	42,725
FY21Q2	42,157
FY21Q3	50,387
FY21Q4	41,156
FY22Q1	46,121
FY22Q2	47,855



Denied/Revoked





Report Date: 4/1/2022
OPR: DCSA ADJ Metrics Team

Vetting Risk Operations Industry Update

PSI Execution

1M
NISP Contractors With Clearance Eligibility

100k
Requests for Investigations Processed
*Interim determinations average 7 days

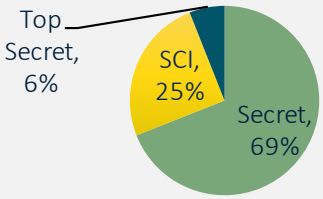
8,000
Incidents Triaged

CV Execution

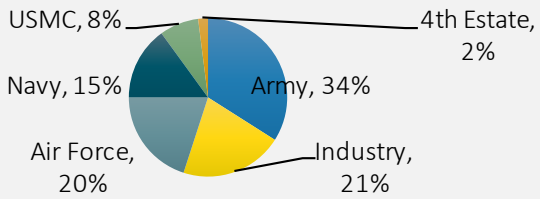
Over 975,000
Industry Subjects Enrolled in CV

~156,000
Industry PRs Deferred into CV to Date

CV Population by Eligibility



CV Population by Component



Industry Reminders

CV ENROLLMENT : WHAT CAN INDUSTRY DO
Submit updated SF86 data if requested!
**Follow guidance posted on DCSA website on Jan. 18, 2022*

FY22 INDUSTRY CV ALERT TRENDS
19K Valid Alerts
8K Actionable
**41% not previously known*
7K Unique Subjects

Majority Criminal and Financial

CV WAY AHEAD
TW 1.25 to TW 1.5

***Educate, Educate, Educate!**
ADVERSE INFO REPORTING

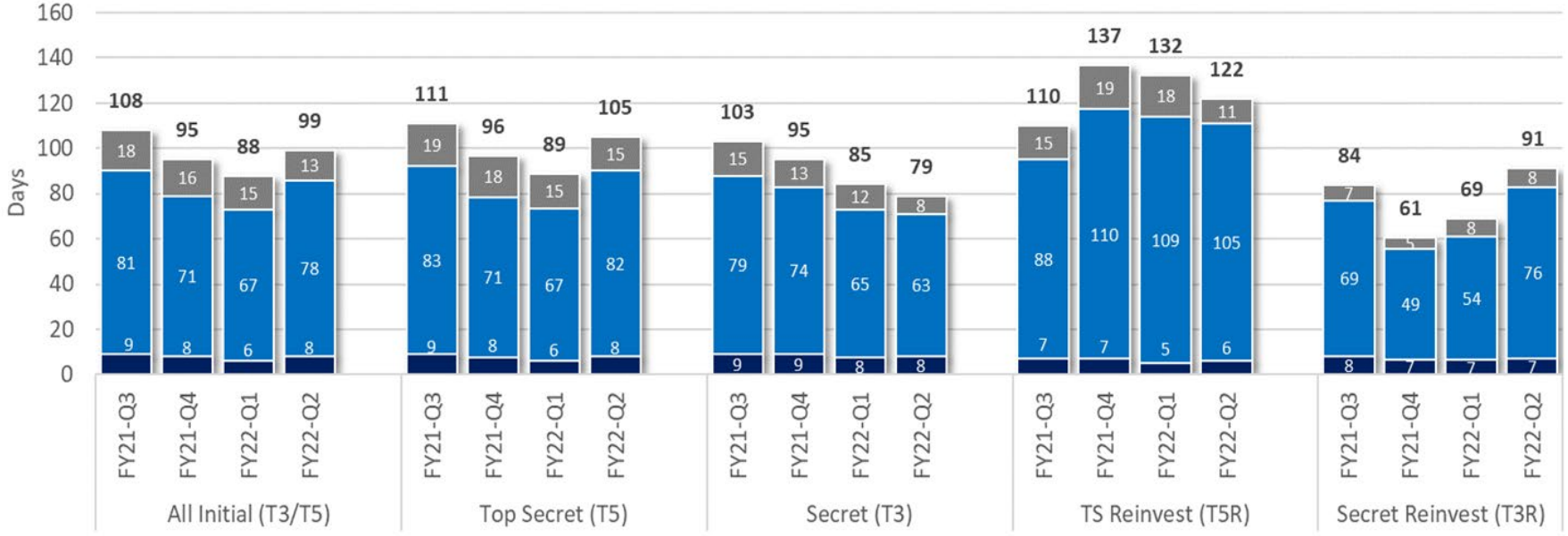
Workload & Timeliness Performance Metrics

Department of Energy

*Metrics provided by Defense Counterintelligence and Security Agency

Quarterly DOE Timeliness Performance Metrics

Average Days for Fastest 90% of Reported Clearance Decisions Made

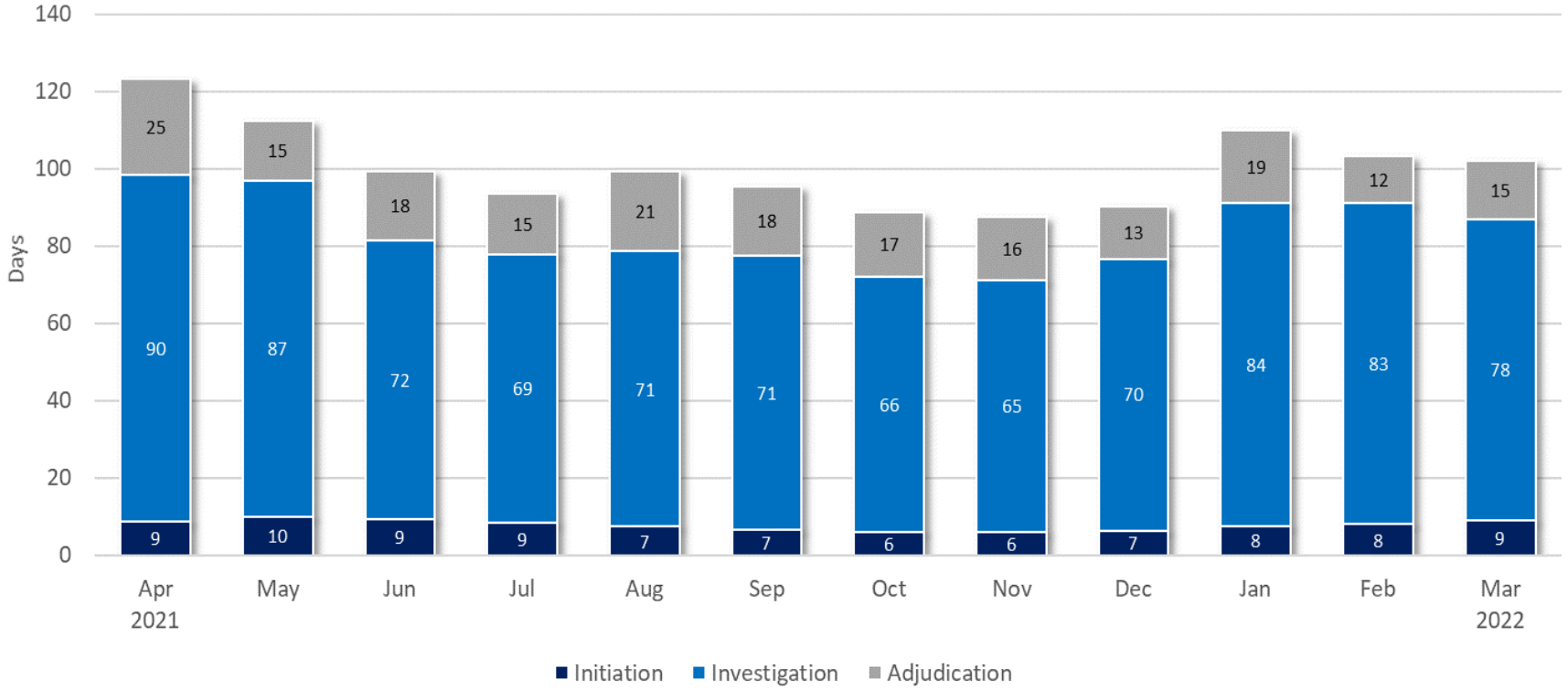


	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations	Secret Reinvestigations
Adjudication actions reported – 3rd Q FY21	2,700	2,206	494	2,632	462
Adjudication actions reported – 4th Q FY21	2,908	2,281	627	2,248	428
Adjudication actions reported – 1st Q FY22	2,797	2,225	572	1,256	390
Adjudication actions reported – 2nd Q FY22	2,718	2,143	575	1,461	708

Data representative of DOE Contractor investigations

UNCLASSIFIED

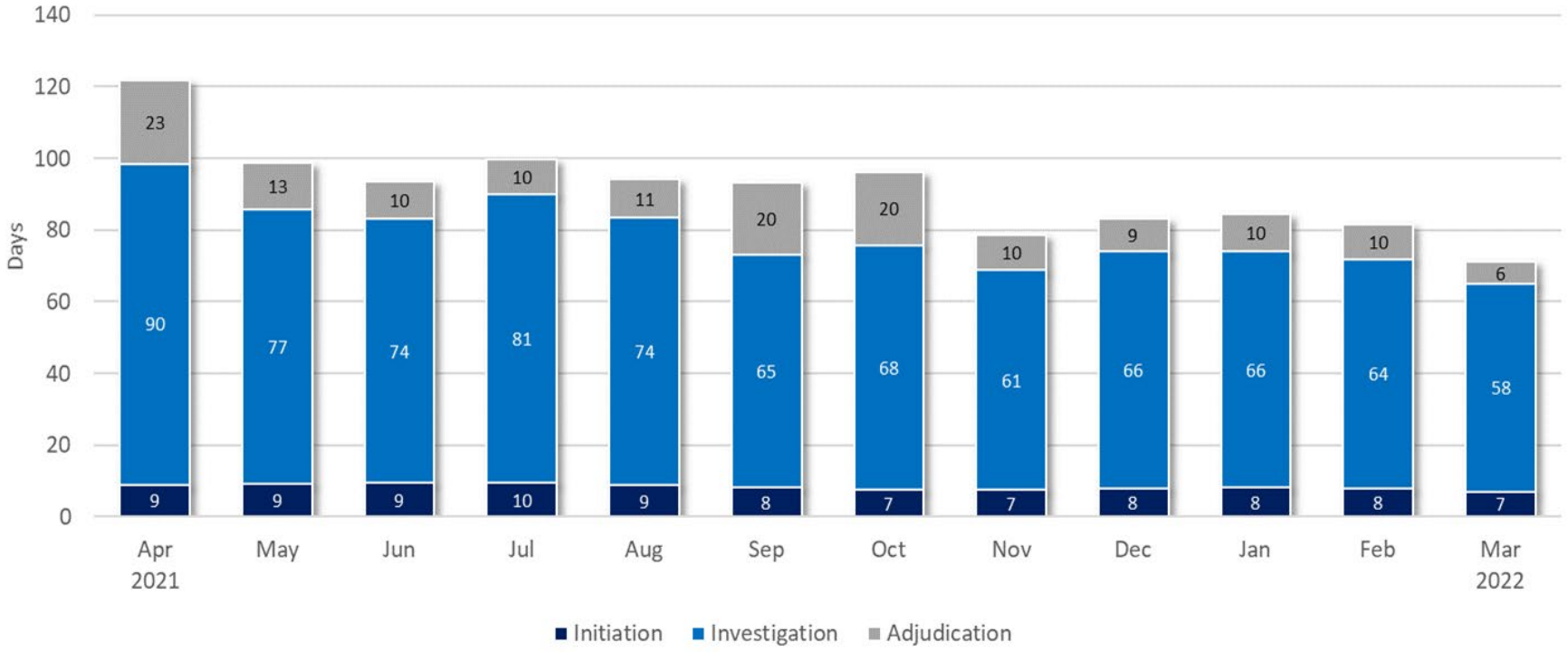
Monthly Timeliness for Fastest 90% of Initial Top Secret (T5) Security Clearance Decisions



	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021	Sep 2021	Oct 2021	Nov 2021	Dec 2021	Jan 2022	Feb 2022	Mar 2022
Total Adjudications Reported	776	625	805	749	718	808	751	747	727	683	626	834
End-to-End Timeliness (Fastest 90%)	123 days	112 days	99 days	93 days	99 days	95 days	89 days	87 days	90 days	110 days	103 days	102 days

Data representative of DOE Contractor investigations

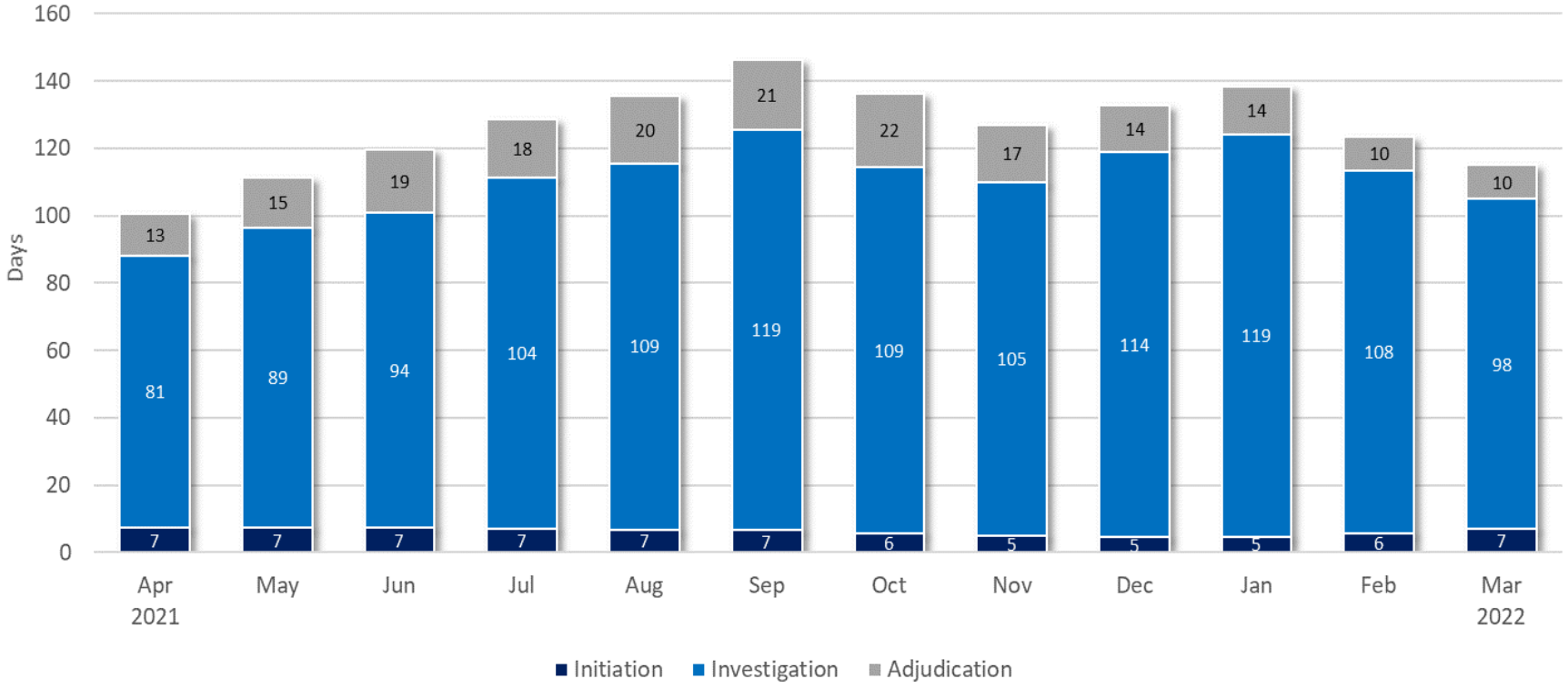
Monthly Timeliness for Fastest 90% of Initial Secret (T3) Security Clearance Decisions



	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021	Sep 2021	Oct 2021	Nov 2021	Dec 2021	Jan 2022	Feb 2022	Mar 2022
Total Adjudications Reported	152	148	194	211	212	203	176	197	199	191	164	220
End-to-End Timeliness (Fastest 90%)	122 days	99 days	93 days	101 days	94 days	93 days	96 days	79 days	83 days	84 days	82 days	71 days

Data representative of DOE Contractor investigations

Monthly Timeliness for Fastest 90% of Top Secret Reinvestigation (T5R) Security Clearance Decisions

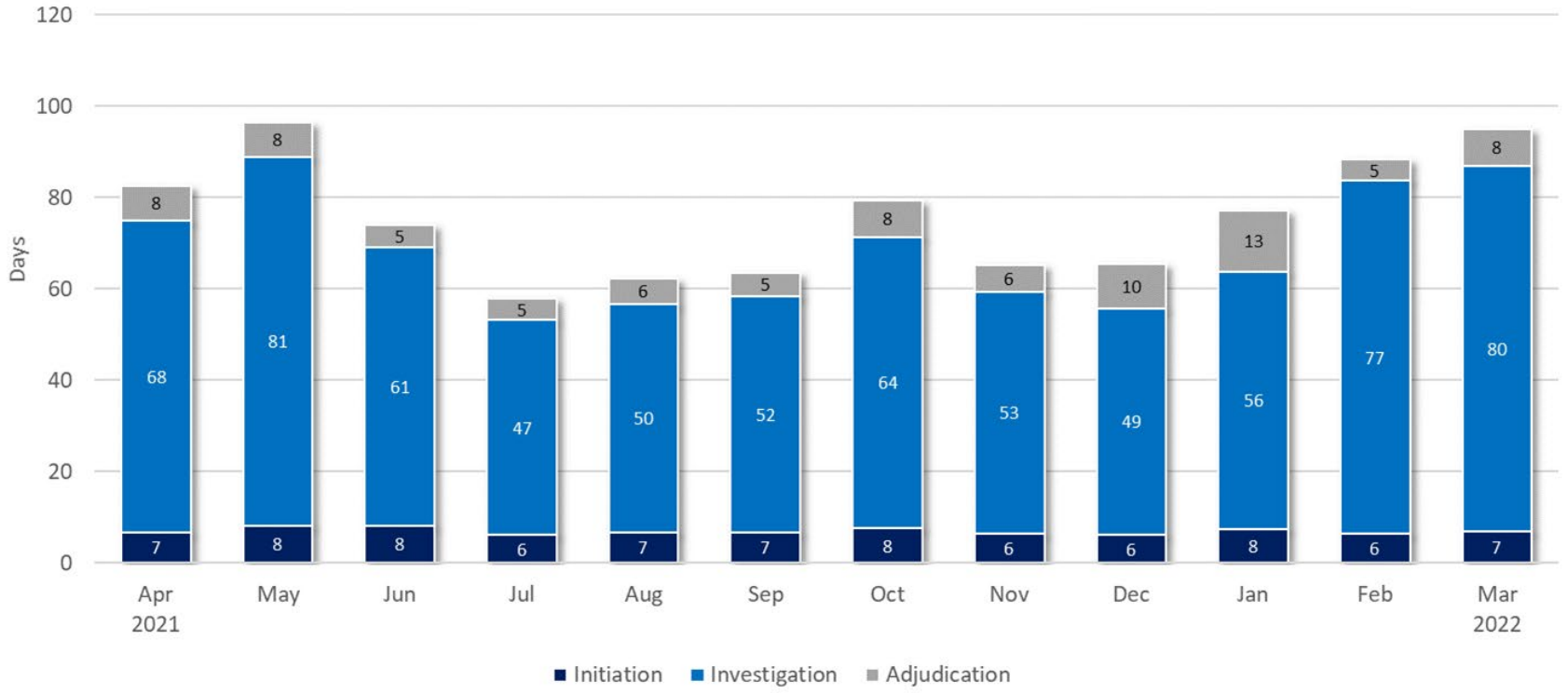


	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021	Sep 2021	Oct 2021	Nov 2021	Dec 2021	Jan 2022	Feb 2022	Mar 2022
Total Adjudications Reported	861	910	861	781	744	721	568	367	321	338	440	683
End-to-End Timeliness (Fastest 90%)	101 days	111 days	120 days	129 days	136 days	146 days	136 days	127 days	133 days	138 days	123 days	115 days

Data representative of DOE Contractor investigations

UNCLASSIFIED

Monthly Timeliness for Fastest 90% of Secret Reinvestigation (T3R) Security Clearance Decisions

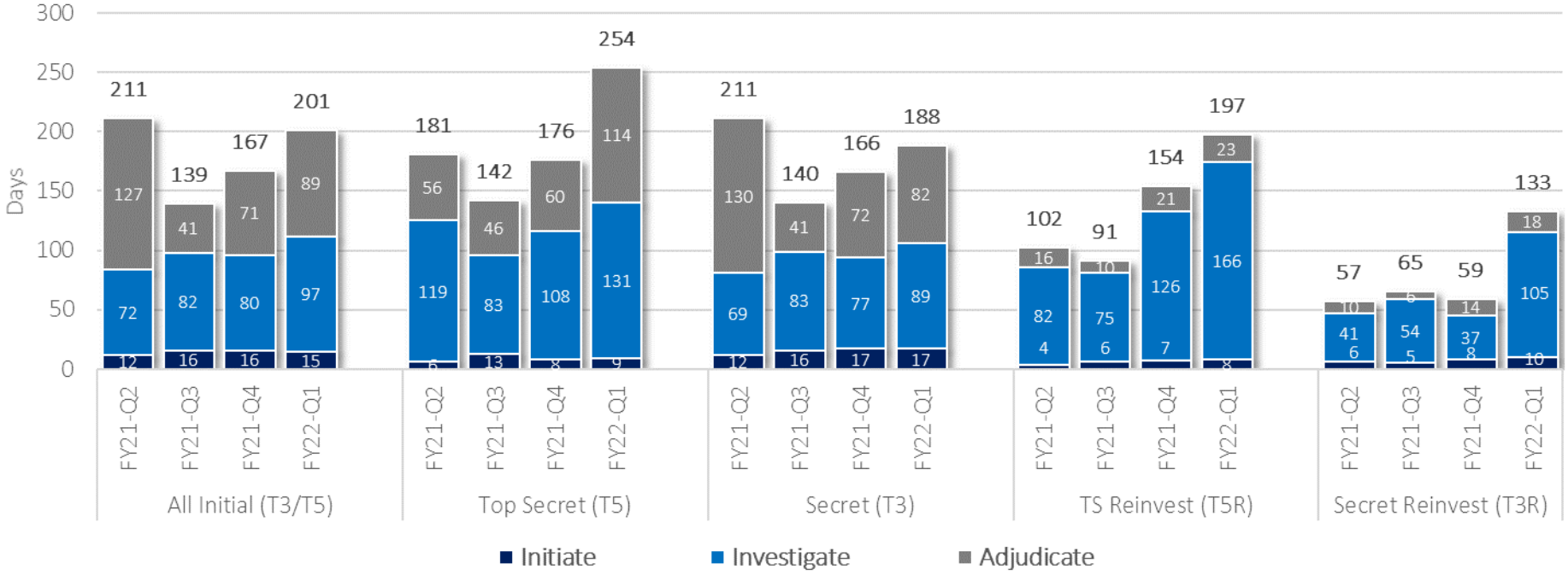


	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021	Sep 2021	Oct 2021	Nov 2021	Dec 2021	Jan 2022	Feb 2022	Mar 2022
Total Adjudications Reported	196	106	160	148	164	117	116	151	123	113	162	433
End-to-End Timeliness (Fastest 90%)	83 days	97 days	74 days	58 days	63 days	63 days	79 days	65 days	65 days	77 days	88 days	95 days

Data representative of DOE Contractor investigations

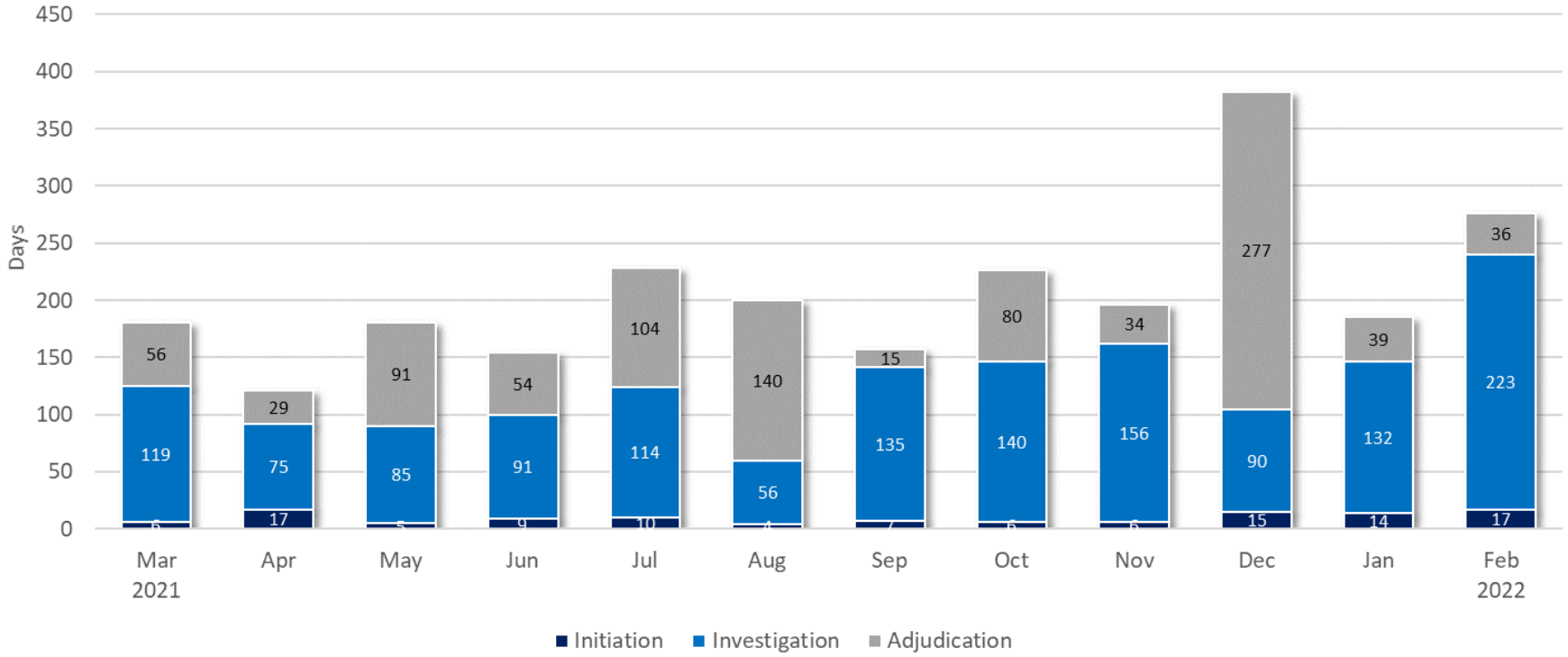
Workload & Timeliness Performance Metrics

Quarterly NRC Timeliness Performance Metrics



	All Initial	Top Seret	Secret/ Confidential	Top Secret Reinvestigations	Secret Reinvestigations
Adjudication actions reported– 2nd Q FY21	82	3	79	16	35
Adjudication actions reported– 3rd Q FY21	86	12	74	44	55
Adjudication actions reported– 4th Q FY21	97	9	88	30	105
Adjudication actions reported– 1st Q FY22	61	12	49	9	58

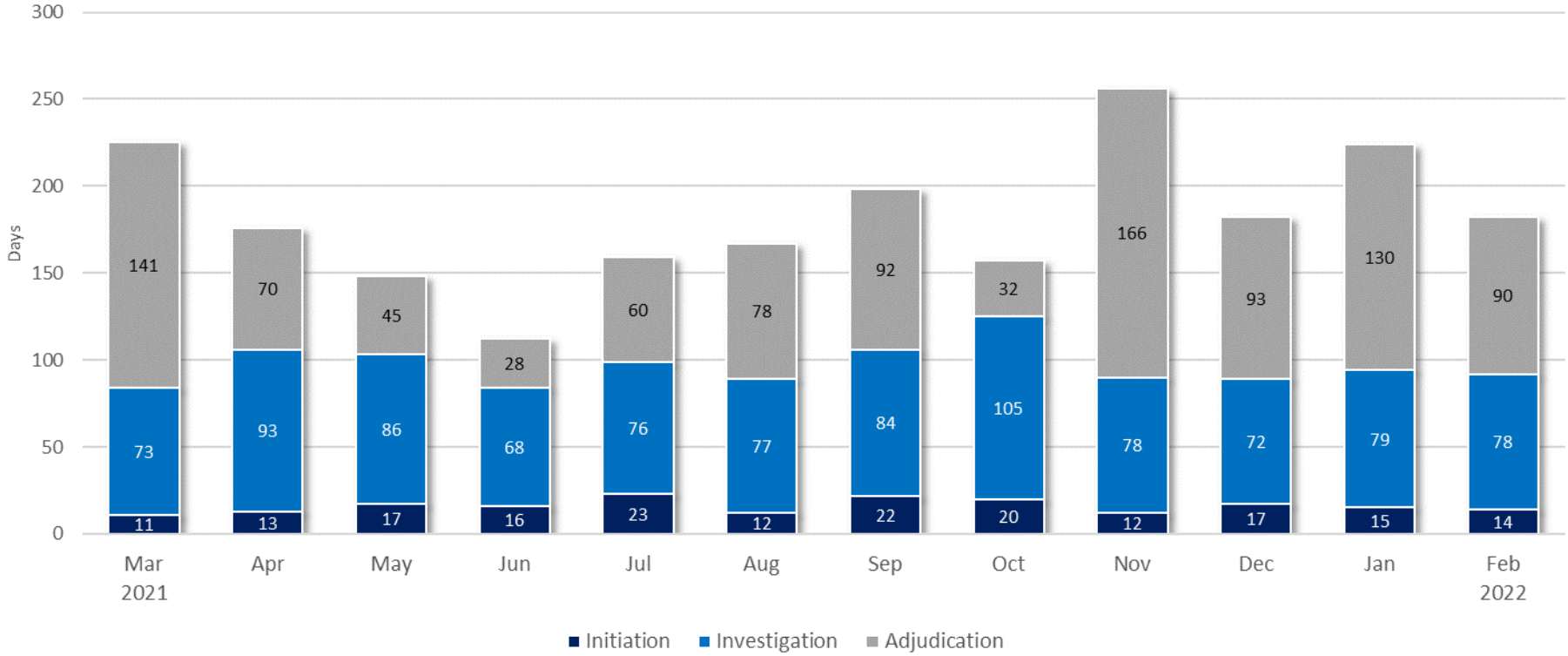
Monthly Timeliness for Fastest 90% of Initial Top Secret (T5) Security Clearance Decisions



GOAL: Initiation – 14 days *Investigation – 80 days* *Adjudication – 20 days*

	Mar 2021	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021	Sep 2021	Oct 2021	Nov 2021	Dec 2021	Jan 2022	Feb 2022
Total Adjudications Reported	3	5	1	6	4	3	2	2	5	5	5	4
End-to-End Timeliness (Fastest 90%)	181 days	121 days	181 days	154 days	228 days	200 days	157 days	226 days	196 days	382 days	185 days	276 days

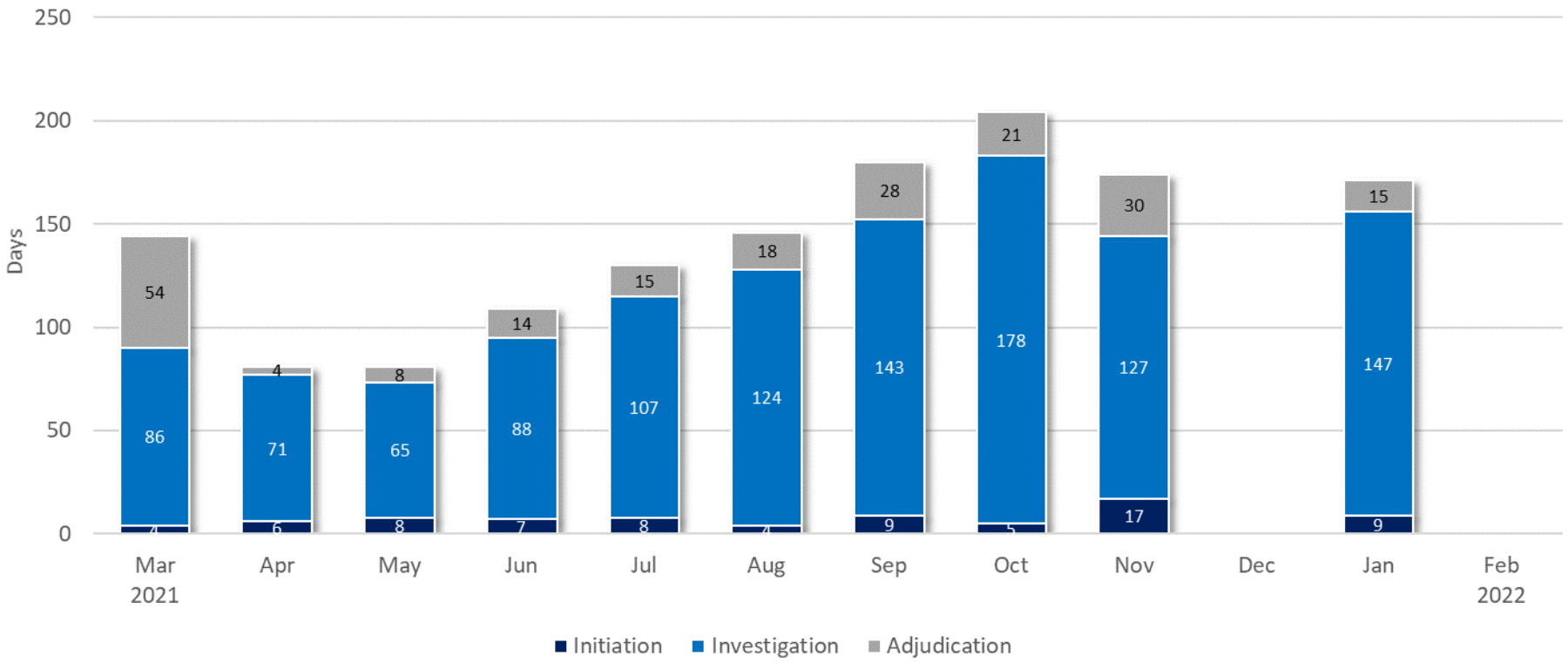
Monthly Timeliness for Fastest 90% of Initial Secret (T3) Security Clearance Decisions



GOAL: Initiation – 14 days *Investigation – 80 days* *Adjudication – 20 days*

	Mar 2021	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021	Sep 2021	Oct 2021	Nov 2021	Dec 2021	Jan 2022	Feb 2022
Total Adjudications Reported	48	22	24	27	38	31	15	17	12	19	30	30
End-to-End Timeliness (Fastest 90%)	225 days	176 days	149 days	112 days	159 days	167 days	198 days	157 days	256 days	182 days	224 days	182 days

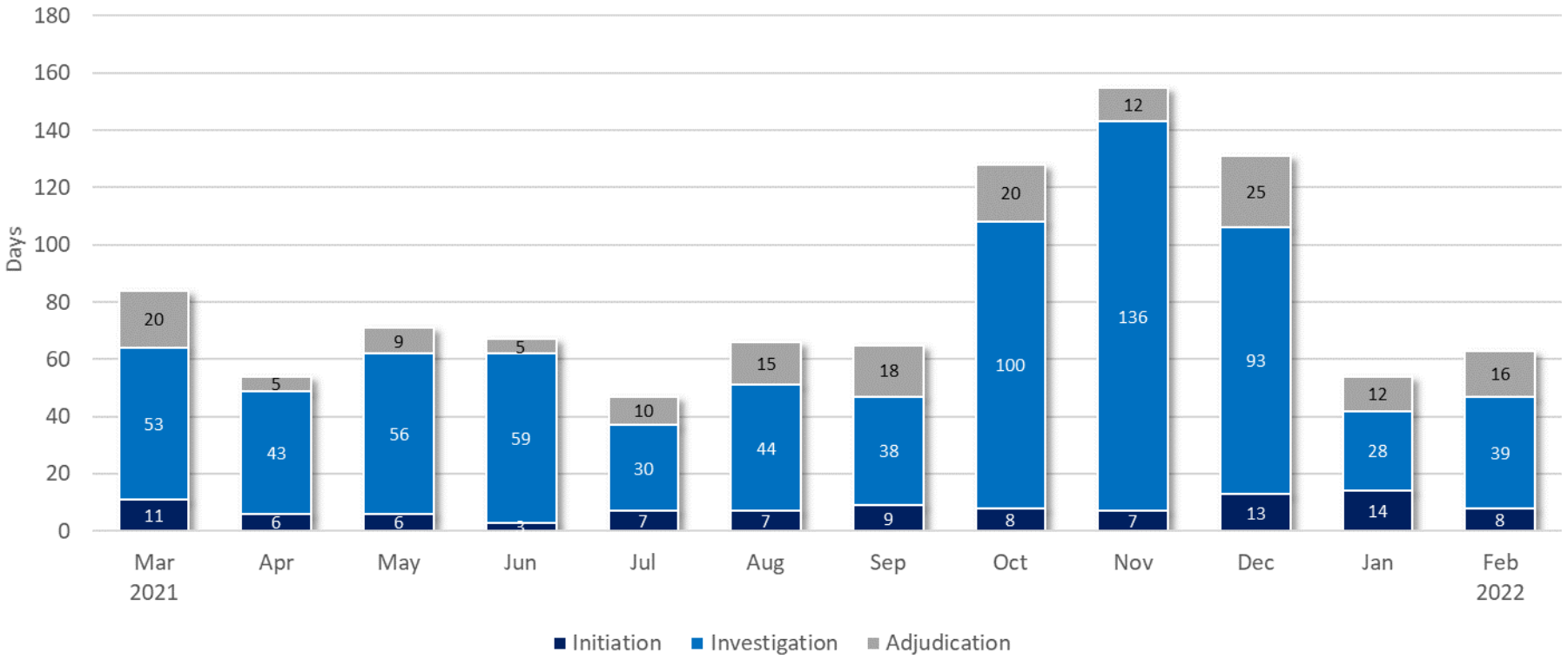
Monthly Timeliness for Fastest 90% of Top Secret Reinvestigation (T5R) Security Clearance Decisions



GOAL: Initiation – 14 days *Investigation – 80 days* *Adjudication – 20 days*

	Mar 2021	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021	Sep 2021	Oct 2021	Nov 2021	Dec 2021	Jan 2022	Feb 2022
Total Adjudications Reported	11	11	15	17	9	8	13	7	2	0	2	0
End-to-End Timeliness (Fastest 90%)	144 days	80 days	80 days	109 days	129 days	146 days	180 days	204 days	174 days	n/a	171 days	n/a

Monthly Timeliness for Fastest 90% of Secret Reinvestigation (T3R) Security Clearance Decisions



GOAL: Initiation – 14 days *Investigation – 80 days* *Adjudication – 20 days*

	Mar 2021	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021	Sep 2021	Oct 2021	Nov 2021	Dec 2021	Jan 2022	Feb 2022
Total Adjudications Reported	8	13	17	25	34	38	33	22	9	27	36	9
End-to-End Timeliness (Fastest 90%)	83 days	54 days	71 days	67 days	47 days	66 days	65 days	128 days	155 days	131 days	54 days	63 days

NISPPAC

Biographies

NISPPAC Designated Federal Officer (DFO) Biographies

MARK BRADLEY. The President of the United States approved Mr. Bradley's appointment as Director of the Information Security Oversight Office (ISOO), effective December 2016. ISOO is responsible to the President for policy and oversight of the government-wide security classification system under Executive Order 13526, the National Industrial Security Program under Executive Order 12829, as amended, and the Controlled Unclassified Information Program under Executive Order 13556. As the Director of ISOO, Mr. Bradley serves as the Executive Secretary of the Interagency Security Classification Appeals Panel and the Public Interest Declassification Board, and as the Chairman of the National Industrial Security Program Policy Advisory Committee, the State, Local, Tribal, and Private Sector Policy Advisory Committee, and the Controlled Unclassified Information Advisory Council. Mr. Bradley has been a member of the Federal government's Senior Executive Service since 2003.

Mr. Bradley previously served as the Director of FOIA (Freedom of Information Act), Declassification, and Pre-publication Review, National Security Division, Office of Law and Policy at the Department of Justice (DOJ). While at the Department, he also served as the Deputy Counsel for Intelligence Policy, and the Acting Chief for Intelligence Oversight.

Before joining the Department of Justice in November 2000, Mr. Bradley served as a CIA intelligence officer and Senator Daniel Patrick Moynihan's legislative assistant for foreign affairs and intelligence matters and as his last legislative director. He co-drafted the legislation that established the Public Interest Declassification Board. Mr. Bradley, who remains a member of the District of Columbia Bar, has also worked as a criminal defense lawyer in the District of Columbia defending indigents accused of serious crimes.

The Society for History in the Federal Government awarded A Very Principled Boy, his biography of Soviet spy Duncan Lee, its 2015 George Pendleton Prize for being the best book written by a federal historian in 2014.

Mr. Bradley is a Phi Beta Kappa graduate of Washington & Lee University and holds an M.A. in Modern History from Oxford University, which he attended as a Rhodes Scholar, and a J.D. from the University of Virginia.

Greg Pannoni

Greg became an employee of the federal government in June of 1980 with the Defense Investigative Service, a component of the Department of Defense. He was initially employed as a personnel security specialist wherein he managed background investigations for the purpose of determining a person's eligibility to access classified national security information. In July of 1983 he transferred to the Defense Industrial Security Program (DISP) and served in a number of positions to include Industrial Security Representative, staff officer and supervisor. Each of these assignments involved responsibilities pertinent to the implementation, monitoring, oversight and policy of the National Industrial Security Program (NISP), the successor to the DISP. He also served as a member of the United States Security Policy Board Staff wherein he worked on information, personnel, physical and industrial security issues, and he was a Deputy Inspector General (IG) within the DSS, Office of the IG for several years.

In December of 2004 Greg joined the staff of the Information Security Oversight Office (ISOO) and currently serves as an Associate Director. ISOO is established within the National Archives and acts in consultation with the National Security Advisor in developing policies and overseeing agency actions to ensure compliance with the President's program for classifying, safeguarding and declassifying national security information per Executive Order 13526. He is responsible for monitoring and overseeing the implementation of this program and the complementary programs for Industry, the NISP per Executive Order 12829, and for State, Local, Tribal and Private Sector Entities, the SLTPS program per Executive Order 13549. As ISOO has been delegated as the Controlled Unclassified Information (CUI) Executive Agent, Greg is responsible for directing the CUI program as well. He is also ISOO's representative to various governance entities to ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security.

He is a Magna Cum Laude graduate of Towson University in Towson, MD, with a degree in Political Science. His is the author of a publication in the Towson University Journal of International Affairs entitled, "Overthrow of Allende: An Analysis of U.S. Involvement."

Greg is a native of Maryland and continues to reside there along with his spouse, two sons, and daughter.

NISPPAC Government Biographies

Valerie B. Kerben

National Counterintelligence and Security Center

Office of the Director of National Intelligence

Current Position: With almost 33 years of federal service, Ms. Kerben holds the position of Senior Security Advisor for the Special Security Directorate at the National Counterintelligence and Security Center (NCSC) since September 2016. In this capacity, she serves as the advisor for all personnel security policy matters for the Director of NCSC and for the DNI in her role as Security Executive Agent (SecEA). She leads the reform efforts in support of the SecEA authorities to develop, implement, and integrate joint security and suitability initiatives with our U.S. Government partners for effective, efficient, and uniform policies and procedures in conducting investigations and adjudications for eligibility for access to classified information or to hold a sensitive position.

Ms. Kerben also serves as the principal liaison for the Performance Accountability Council initiatives and is an active participant in personnel security working groups, prepares briefing materials for internal and external Hill engagements and presents at many public and private sector forums. She has been selected as the DNI primary representative for the National Industrial Security Program and Policy Advisory Council (NISPPAC) and for the State, Local, Tribal and Private Sector Policy Advisory Council (SLTPS).

Past Experiences: Previously from May 2005-September 2016, Ms. Kerben was employed at the U.S. Nuclear Regulatory Commission (NRC) and for seven years, Ms. Kerben served as Chief of Personnel Security Branch. She was responsible for the operations and management of the centralized personnel security and Drug-Free Workplace programs including end-to-end security processing and rendering national security clearance and access determinations for federal, contractor and licensee employees.

Prior to joining the NRC, she worked at the U.S. Department of Justice, Immigration and Naturalization Service (INS) as a Personnel Security Specialist, responsible for policy and training and adjudicative functions. While at INS, she was nominated to the position of Chair of the Adjudicator Training Subcommittee at the U.S. Security Policy Board.

In 1988, she began her federal career with the U.S Office of Personnel Management (OPM), Washington Federal Investigative Services as a Federal Investigator. She was assigned to conduct full field background investigations for a myriad of Executive branch agencies and for various positions within the White House and on Capitol Hill. Additionally, she held many career enhancing positions such as Recruiter and Branch Chief of Student Investigator Cooperative Education Program.

Ms. Kerben obtained her B.A. in Criminology from University of Maryland, College Park. She resides in Maryland with her husband and has two college age daughters.

Tracy L. Kindle

U.S. Department of Energy
Personnel Security Policy Program Manager

Mr. Kindle is originally from Florida and now resides in Maryland. Mr. Kindle spent 20 years in the U.S. Army, retiring in 2005. He has held a number of positions as a civilian security specialist in various Department of Defense (DoD) agencies. After retiring from the Army, Mr. Kindle spent two and a half years as a Security Officer with the U.S. Army from 2005-2008; Information Security Specialist with the Defense Threat Reduction Agency in 2008; Industrial Security Specialist (Policy) with the Defense Counterintelligence and Security Agency formerly Defense Security Service from 2008-2013; Security Education, Training and Awareness and Information Security Supervisory Security Specialist with the Department of the Navy from 2013 to 2018. Mr. Kindle obtained four DoD Security Professional Education Development certifications and holds a Master's of Science Degree in Human Resources Development and Management from National Louis University. As the Department of Energy (DOE) Personnel Security Policy Program Manager, Mr. Kindle has the primary responsibility for assessing, clarifying, and developing DOE-wide Personnel Security Program policy. Mr. Kindle is the DOE alternate voting member on the National Industrial Security Program Policy Advisory Committee and the State, Local, Tribal, and Private Sector Policy Advisory Committee.

Rich DeJausserand serves as the Deputy Director for the Department of Homeland Security (DHS), Office of the Chief Security Officer (OCSO), National Security Services Division (NSSD), Industrial Security Program. In his role as the Deputy Director, Rich is responsible for the Departmental level protection of National Security Information, Technology, Personnel and Facilities.

Prior to assuming the Deputy Director position, he served as the DHS OCSO Compliance/Standards & Training Division Branch Chief (2015-2019), responsible for oversight of the Classified National Security Information Program for State, Local, Tribal and Private Sector entities. He also served as the DHS Science & Technology (S&T) Security Deputy Branch Chief (2011-2015), responsible for Physical Security and the Security Compliance Review program providing security support for the S&T Directorate and five National Research Laboratories.

Rich DeJausserand retired from the United States Navy and served as a Chief Petty Officer (1998-2008). He is a native of the Great State of Michigan and holds both a Masters and Bachelors Degree in Criminal Justice Administration from Columbia Southern University, Orange Beach, Alabama.

Keith Minard currently serves as the Senior Policy Advisor within the Critical Technology Protection Directorate of the Defense Counterintelligence and Security Agency (DCSA). In this role he provides policy support for DCSA leadership and staff, government, and industry partners in support of the CTP security mission that include National Industrial Security Program, SCIF Accreditation, Controlled Unclassified Information, and other key mission areas. His prior assignments include serving with the Office of the Under Secretary of Defense for Intelligence and Security, where he managed Physical Security Policy for DoD, the U.S. Army at Fort Belvoir where he served as the installation, Chief of Physical Security, and served in the United States Army as a Military Policeman for over 20-years. His professional security certifications include SFPC; SAPPC; SPIPC; Industrial Security Oversight Certification; and Physical Security Certification. His education includes a Bachelor of Arts degree in Security Management and Master of Arts degrees in Business and Organizational Security Management, and Procurement and Acquisition Management from Webster University.

Matthew Roche
Defense Counterintelligence and Security Agency (DCSA)
Critical Technology Protection (CTP)

Matthew currently serves as the CTP, Operations Division Chief, DCSA Headquarters, Russell Knox Building, Quantico Marine Base, VA. As the CTP Operations Chief he is responsible for providing the CTP Regional Directors the tactics and tools required for implementing the National Industrial Security Program.

Matthew joined DCSA in May 2002. He has 26 years' experience supporting the Department of Defense. Prior to his current position he's served in multiple capacities in DCSA including Industrial Security Field Operations, Chief of Staff, Industrial Security Program Integration Program Manager, Field Office Chief, Senior Staff Action Officer, Arms Ammunition and Explosives Program Manager, Industrial Security Representative, and Personnel Security Investigator.

Matthew completed the Leadership in a Democratic Society Program, Federal Executive Institute, Charlottesville, VA — 2017, Executive Leadership, Harvard Kennedy School, Cambridge, MA — 2014, Bachelor of Arts, California University of Pennsylvania, California, PA — He is a US Army veteran where he served as an airborne infantryman. The Army awarded Matt an Army Commendation Medal for his service. Matt earned a Bachelor of Arts degree in Political Science from California University of Pennsylvania, California, Pennsylvania in 1994.

Elizabeth O'Kane

Senior Security Advisor,
Counterintelligence, Human Intelligence, Foreign Disclosure, & Security Directorate
Office of the Deputy Chief of Staff for Intelligence, G-2
Headquarters, Department of the Army

As the Army's Senior Security Advisor, Elizabeth manages the policy, political, programmatic, and technical challenges confronting the Army's security portfolio. She also served the Army G-2 as the Chief of Personnel Security, advocating for swift personnel vetting reform. Prior to the Army, she worked at the Office of the Under Secretary of Defense for Intelligence & Security as the Department's lead for Continuous Evaluation. During this time, Elizabeth also oversaw the directorate's budget, executed numerous contracts, and made key contributions to the insider threat and the personnel, information, and physical security teams. Elizabeth began her federal career in a developmental position with the Defense Information Systems Agency (DISA). While at DISA, Elizabeth served in several positions and gained diverse experience in information technology, data analysis, human resources, consulting, program management, policy, and acquisition. Elizabeth obtained both her bachelor's and master's degrees from Indiana University's School of Public and Environmental Affairs in Bloomington, Indiana. She continued her passion for learning by completing both the DoD and the DISA Executive Leadership Development Programs and achieving a Chief of Information Operations Certificate from the National Defense University. Elizabeth has received formal recognition throughout her career for individual and team performance as well as risk-taking. Elizabeth prides herself on building teams that promote innovation, creativity, and diversity in the workplace. She is happiest enjoying the outdoors and spending time with her husband and three children.

JENNIFER M. AQUINAS

Jennifer M. Aquinas, a member of the Senior Executive Service, is the Director of Security, Special Program Oversight and Information Protection, Office of the Administrative Assistant, Office of the Secretary of the Air Force, Arlington, Virginia.

Ms. Aquinas served as an officer on active and reserve Air Force from 1996 to 2016 in a variety of Security Forces assignments. She entered federal civil service in 2008 with the Office of the Secretary of Defense for Intelligence. She transferred to the Department of the Air Force in 2013 and was instrumental in standing up the Air Force Counter Insider Threat program and leading Department of Defense efforts in personnel vetting and security reform. She was appointed to the Senior Executive Service in 2020 as the Deputy Director, Security Special Program Oversight and Information Protection.

In her current position, she provides security leadership, policy direction, integration and oversight of the Department of the Air Force's Special Access Programs and Information Protection Enterprise to protect the nation's most sensitive information, technologies and capabilities. In this capacity, she is also the Functional Manager for the Department of the Air Force's more than 2,000-member civilian security community.

EDUCATION
1996 Bachelor of Science, Criminal Justice, Pace University, New York
2001 Squadron Officer School, Air University, Maxwell Air Force Base, Ala.
2002 Master of Arts, Business and Organizational Security Management, Webster University, St. Louis
2010 Master of Military Operational Art and Science, Maxwell AFB, Ala.
2017 Master of Arts, National Security and Resource Strategy, Fort Lesley J. McNair, Washington, D.C.

CAREER CHRONOLOGY
1. 1996–1998, Flight Leader, 10th Missile Squadron, Great Falls, Mont.
2. 1998–1999, Flight Commander, 341st Missile Squadron, Great Falls, Mont.
3. 1999–2000, Flight Commander, 11th Security Forces Squadron, Bolling Air Force Base, Washington, D.C.
4. 2000–2002, Flight Commander, Detachment 1, 11th Security Forces Squadron, the Pentagon, Arlington, Va.
5. 2002–2016, Commander, U.S. Air Force Reserve (various assignments)
6. 2002–2008, Contractor, Department of Defense, the Pentagon, Arlington, Va.
7. 2008–2013, Security Specialist, Office of the Under Secretary of Defense for Intelligence, the Pentagon, Arlington, Va.
8. 2013–2015, Program Manager, Office of the Administrative Assistant to the Secretary of the Air Force, the Pentagon, Arlington, Va.
9. 2015–2016, Division Chief, Strategy, Readiness and Force Development, Directorate of Security Forces, the Pentagon, Arlington, Va.
10. 2016–2017, Student, Eisenhower School, National Defense University, Washington, D.C.
11. 2017–2020, Division Chief, Security Policy and Oversight, Office of the Administrative Assistant to the Secretary of Air Force, the Pentagon, Arlington, Va.
12. 2020–2022, Deputy Director, Security, Special Program Oversight and Information Protection, the Pentagon, Arlington, Va.
13. 2022–present, Director, Security Special Program Oversight and Information Protection, the Pentagon, Arlington, Va.

AWARDS AND HONORS
Air Force Meritorious Civilian Service Award
Meritorious Service Medal
Air Force Commendation Medal
Air Force Achievement Medal
National Defense Service Medal
Global War on Terrorism Service Medal
Nuclear Deterrence Operations Service Medal with "N" device
Armed Forces Reserve Medal

(Current as of March 2022)

ACTING DEPUTY ASSISTANT SECRETARY FOR

INTELLIGENCE AND SECURITY

Richard L. Townsend

Richard L. Townsend is the Director for Security at the U.S. Department of Commerce. Headquartered in the Herbert C. Hoover Building in Washington D.C., Mr. Townsend is responsible for a nationwide, multi-disciplined security program, that includes: personnel security, physical security, law enforcement, information security, and continuity and emergency management. Mr. Townsend serves as a primary member of the National Industrial Security Program Policy Advisory Committee (NISPPAC), the primary Departmental Representative to the DHS Interagency Security Committee (ISC), the Federal Law Enforcement Training Centers (FLETC) Training Partner and is the Delegated Original Classification Authority (Secret Level) for the Department. Since January 2021, has been the Acting Deputy Assistant Secretary for Intelligence and Security. In this capacity, in addition to leading the Office of Security, he also oversees the Department's Investigations and Threat Management Service and the Office of Intelligence.

Mr. Townsend previously served as the Director of the Office of Facilities and Environmental Quality overseeing Departmental policy, programs, and operational functions. In this position he served as the Department's Senior Real Property Officer (SRPO) and was a member of the Office of Management and Budget's Federal Real Property Council. Additionally, as a part of his energy and environmental management oversight role, he served as the Deputy Chief Sustainability Officer (Deputy CSO) for the Department and had operational, support, and maintenance responsibility for the Commerce Headquarters building; including overseeing the Herbert C. Hoover Building Renovation and Modernization Project on behalf of the Department.

Prior to joining the Department, Mr. Townsend has held leadership and senior management roles in both the private and public sectors. In the public sector, working for the Department of Defense based at the Pentagon, he supported the programmatic needs for the Office of the Secretary of Defense, the Military Departments, Defense Agencies and Field Activities. In the private sector, Mr. Townsend has held senior positions at General Dynamics, Booz Allen Hamilton, and Parsons Corporation supporting clients such as the U.S. Missile Defense Agency, the U.S. State Department's Overseas Building Office, and the U.S. Intelligence Community.

Mr. Townsend earned his Bachelor of Architecture degree from Carnegie Mellon University in Pittsburgh, PA.

NISPPAC Industry Biographies

HEATHER M. SIMS

Mrs. Heather Sims provides Strategic Industrial Security advice for the Chief Security Officer at L3Harris, headquartered in Melbourne, Florida. Her primary responsibility is to provide subject matter expertise for a variety of security disciplines throughout the L3Harris enterprise.

Ms. Sims is also the current Industry Spokesperson to the National Industrial Security Program Policy Advisory Committee (NISPPAC). NISPPAC members advise on all matters concerning the policies of the National Industrial Security Program, including recommending changes. The NISPPAC serves as a forum to discuss policy issues in dispute.

Prior to her arrival at L3Harris, Mrs. Heather Sims was the Strategic Security Advisor to the General Dynamics Chief Security Officer. Prior to her arrival in cleared industrial, Heather was the Assistant Deputy Director for Industrial Security Field Operations at the former Defense Security Service, now Defense Counterintelligence and Security Agency located in Quantico, Virginia. Mrs. Sims was responsible for the day-to-day field operations throughout the United States and was an instrumental liaison to other government agencies and cleared contractors. Prior to assuming the role of Assistant Deputy Director, she was the St. Louis Field Office Chief, responsible for supporting approximately 700 facilities in Missouri, Illinois, Wisconsin, Indiana, Minnesota, and Iowa. Mrs. Sims last role with DSS was a special Department of Defense project on behalf of the Secretary of Defense researching and preparing a Congressional response to The National Defense Authorization Act for Fiscal Year 2017 Section 951, ultimately bringing the security investigation mission back to the department for the federal government.

Prior to her employment with DSS, Mrs. Sims was the Chief, Plans and Programs, 375 Security Forces Squadron, Scott Air Force Base, Illinois. Mrs. Sims provided supervision to over 27 staff personnel comprised of civilian, military and contractors. She had program management oversight of the following; Police Service, Installation Security, Physical Security, Electronic Security Systems, Policy and Plans, Installation Constable, Reports and Analysis and Information/Industrial/Personnel Security at an Air Force installation that was home to USTRANSCOM, Headquarters Air Mobility Command, Air Force Communications Agency and three Air Force wings Additionally, Mrs. Sims was responsible for security oversight of 64 geographically separated units spread throughout the United States.

Mrs. Sims holds a Bachelor's degree in Workforce Education and Development from the University Southern Illinois. She is also a graduate of the Excellence in Government Senior Fellows Program and the Federal Executive Institute as well as a recipient of the Distinguished Service Award and the Air Force Exemplary Civilian Service award. Mrs. Sims grew up in Pennsylvania and began her Air Force career in August 1989 as a Law Enforcement Specialist. Following Law Enforcement technical training, she was assigned to various overseas and stateside assignments working a variety of law enforcement and security positions. She lives in Melbourne, Florida with her husband John Sims and two of their three children.

Rosael (*Rosie*) Borrero

Ms. Rosie Borrero is a Cyber GRC Analyst Chief for SAIC; responsible for developing a Program Management Office to support SAIC's Information Assurance and Classified Operation's teams by managing milestones and status of all classified systems, identifying and managing risk, and interfacing with applicable stakeholders to enable SAIC's mission while navigating various customer requirements.

Rosie has over 22 years of experience in the cyber security field. She has held various cyber security positions within industry as well as on active duty in the United States Air Force; supporting various Government agencies across the Intelligence Community and Department of Defense.

Ms. Borrero was elected as a National Industrial Security Program Policy Advisory Committee (NISPPAC) Representative in 2018 and represents industry on the NISPPAC Information Systems Authorization (NISA) Working Group. She also serves as the Chairperson on the Board of Directors for the Community Association for Information System Security Working Group (CAISSWG).

Rosie has a Bachelor of Science degree in Business Administration and a Master of Arts Degree in Business and Organizational Security Management. She has also earned and maintains a CISSP certification.

Cheryl M. Stone

Cell: 202-809-8764
cstone@rand.org

Cheryl M. Stone is the Director, Corporate Security & Safety at RAND Corporation. She provides leadership and direction for the global Security and Safety program covering NISPOM, intelligence, International Travel, and Business Continuity and Disaster Recovery program both domestic and international. She was selected to serve as one of eight industry representatives on the National Industrial Security Program Policy Advisory Committee (NISPPAC) and was nominated to the new Board of Directors for the FFRDC/UARC Security Committee, a MOU signatory to the NISPPAC. She is also the Secretary for the ASIS, Defense and Intelligence Council. Previously, she was the Director of Industrial Security at DynCorp International, LLC from February 2008 to August 2013. She was a Senior Executive and federal employee for over 28 years and retired as the Associate Administrator for Defense Nuclear Security at National Nuclear Security Administration within the Department of Energy in 2008. Other government positions Cheryl served was the Deputy Director for Security at Department of Commerce from March to October 2004, and from February 2000 to March 2004 she guided the personnel security program of the U.S. Nuclear Regulatory Commission (NRC) as the Personnel and Physical Security Branch Chief. Cheryl planned, developed, directed and coordinated implementation of all personnel and physical security policies and activities governing the agencies' nationwide program. She also managed the NRC Criminal History and Drug Testing programs. Prior to the NRC, she was employed by the Department of Navy (DoN) for sixteen years as a Senior Security Specialist and Special Access Program Branch Chief. During that time, she served in the security policy section, where she led four discreet centralized security divisions. They included the DoN Special Access Program Central Adjudication Facility, Security Policy Support, the personnel clearance, access and facility database, and the Security Close-Out division.

Mrs. Stone prepared and oversaw implementation of policies and directives for sensitive national security projects, ensuring compliance with Department of Defense physical, personnel and computer security within the Navy Special Access Program Central Office. During this period, she reengineered personnel and facility security procedures significantly reducing cost and eliminating mismanagement of scarce security resources.

Mrs. Stone established the first Navy SAP Central Adjudication Facility responsible for ensuring compliance with national security policy. She managed the adjudication review process for granting, suspending, revoking, or denying access; ensuring individuals nominated for access to National Security Information were afforded due process. She also oversaw the development and deployment of a Security Management System, a large relational database, populated with over four million records that maintained pertinent security information on classified Navy projects. Her responsibilities included managing the Automated Information System Security Branch, providing computer security oversight and support within the organization as well as field activities.

Mrs. Stone actively participated in several U.S. Security Policy Board sponsored committees and working groups.

Mrs. Stone has a Bachelor of Science degree in Criminal Justice and a Masters degree in Security Management. She began her government career as a Special Agent with the Defense Investigative Service.

Aprille Abbott, ISP©
INDUSTRIAL SECURITY PROFESSIONAL

Aprille Abbott is currently employed by the MITRE Corporation as an Industrial Security Program Lead and Corporate FSO. She has been a security professional for over 20 years' and has had notable success in a broad range of initiatives that provided support to the security community. The most impactful initiatives have involved her active roles in NCMS "Society of Industrial Security Professionals in the following capacities:

- President of the Society 2 years
    - NCMS MOU representative to the NISPPAC
- Vice President 2 years
- Board of Director 9 years
- National Seminar Chair 3 years
- National Program Chair 2 years
- National Chapter Chair Liaison to the NCMS Board of Directors
- New England Chapter Local leadership positions
- Elected to the NISPPAC October 2019

Each of these roles required her to foster working relationships with government and industry partners, demonstrate leadership qualities, work to implement change and attend Government and Industry meetings as the representative for NCMS and Industry.

DEREK W. JONES

Assistant Department Head, Government Security
Security Services Department
Massachusetts Institute of Technology
Lincoln Laboratory

Derek W. Jones serves as the Assistant Department Head for the Security Services Department at MIT Lincoln Laboratory providing direct program support under the Laboratory's Chief Security Officer. Mr. Jones has supported Lincoln Laboratory for almost 17 years serving in a variety of positions to include personnel security, business operations and manager of industrial security.

In his current role, Mr. Jones is directly responsible for security management oversight, guidance and direction for all facets of the Laboratory's industrial security program and special program activities to meet government and contractual security requirements. His responsibility also includes managing the security program for local remote facilities and Laboratory field sites. Mr. Jones serves as a security senior management representative with government sponsors to include the Air Force, DARPA, DCSA, ODNI, etc. Key program oversight aspects include: personnel security, commercial background investigation program, visitor services, education and awareness, vulnerability assessments, closed/secure area administration and construction, policies and procedures, investigations, counterintelligence and insider threat. In addition, he is responsible to manage security fit-up and operational support for remote activities.

Mr. Jones has a long and proven track record providing critical support to a high performing security operation that has been nationally recognized by OUSD. The program at Lincoln Laboratory is dynamic and complex requiring critical skills in leadership, influence and project execution. Mr. Jones was one of the elite selected to participate in MIT's Leadership Program where only two fellows are chosen to attend. He has also received numerous awards for his participation or leadership in a number of efficiency improvements and large scale infrastructure projects. Mr. Jones chairs the FFRDC/UARC Policy Working Group and leads monthly telecoms with the other FFRDC/UARC partners to encourage the sharing of information, best practices and experiences. Mr. Jones is a member of the MIT Lincoln Laboratory Information Technology Security Counsel, teaming with the Chief Information Officer and key IT personnel and leaders within the Laboratory to enable a secure environment to mitigate incidents and deter insider threat.

Mr. Jones received his undergraduate degree in Criminal Justice from Westfield State University, and received his graduate degree in Criminal Justice from the University of Massachusetts Lowell. He has served on the University of Massachusetts Alumni Board upon the personal request from the Criminal Justice program department head.

Tracy Durkin

Mrs. Tracy Durkin is a dedicated security professional with over 30 years of experience in multiple security disciplines across the Intelligence and DoD communities.

Tracy is currently a Vice President in security at ManTech in Herndon, VA. She manages and oversees their Personnel Security Center (PSC), Physical Security team, Security Education Program, Systems Security and the Information Security team.

Tracy was elected as a National Industrial Security Program Advisory Committee (NISPPAC) representative in 2020 and is the representative for industry in the NISPPAC Clearance Working Group. She also serves as the Chairperson on the Board of Directors for the Industrial Security Working Group (ISWG).

Tracy holds a Business Management degree from Strayer University. She is also a Certified Facility Security Officer. Tracy grew up in Maryland and began her security career in 1990 when she became a security officer supporting several Intelligence agencies. She lives in Warrenton, VA with her husband Jared and her two sons. Tracy also has two daughters and five grandchildren.

Greg Sadler, CISSP, CISM
Senior Director, Security

GDIT

Greg Sadler has over 25 years of industrial security experience associated with managing and directing Government contracts. He is currently employed by General Dynamics Information Technology, a leading provider of information technologies and related services within agencies of the Department of Defense, the Intelligence Community, the U.S. Department of State, the U.S. Department of Homeland Security, the U.S. Department of Justice, and other agencies.

As a direct report to the Vice President of Security, Mr. Sadler provides security support to all GDIT Defense business entities worldwide, emphasizing integration of security with core business process. Mr. Sadler has been working for GDIT for over two years with previous engagements with PAE, USIS, TASC, Northrop Grumman, Sprint Nextel and Lockheed Martin.

As a Senior Director of Security, Mr. Sadler oversees security of the 10,000+ employees as well as company assets around the globe. He manages a security staff of over 50 and administers an annual budget in excess of $6 million. Mr. Sadler is responsible for security programs that ensure the safeguarding of classified material and directs a team of professionals that support the security aspects of SCI, Special Access, and DOD security issues.

Mr. Sadler is experienced in all elements of industrial security under the cognizance of Intelligence Community and Department of Defense clients. His expertise includes a history of information systems, physical and personnel security operations as an industry partner. Mr. Sadler has served as a consultant to other companies in development of security programs, security information management, and incident management. Mr. Sadler is a Marine Corps veteran, former Co-Chairman of CAISSWG's DC Chapter, served on the Industrial Security Working Group (ISWG) Board of Directors, holds a BS in Business Administration from Strayer University and is completing an MBA through the Jack Welch Management Institute. He has maintained Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) certifications since 1999 and 2003 respectively.

DAVE TENDER

Chief Security Officer

Dave Tender is ASRC Federal's chief security officer (CSO). As CSO, Dave is responsible for managing security and facility operations including physical and personnel security, clearances and facilities.

Dave is a seasoned security leader with over 25 years of experience. He is deeply skilled in executive security operations leadership and execution, security program development, cyber support, disaster recovery, business continuity, integration activities as well as helping align the company to meet new security compliance requirements. Prior to joining ASRC Federal, Dave was vice president, chief security officer of Perspecta where he led a 100-person enterprise security and emergency operations team and managed Perspecta's Insider Threat program. Additionally, he was the vice president, chief security officer of Vencore, Inc. where he managed a team of 50 employees supporting enterprise security operations and a budget of $4.5 million dollars.

Dave is a board member for the National Industrial Security Program Policy Advisory Committee (NISPPAC) and vice chairman of the Intelligence Security Working Group (ISWG). In his free time, Dave enjoys indoor and outdoor activities with his family.

Dave holds both a bachelor's and master's degree in security management from American Military University.

NISPPAC Speaker Biographies

Peregrine D. Russell-Hunter
Director
Defense Office of Hearings & Appeals (DOHA)

As the Director of the Defense Office of Hearings & Appeals, Mr. Russell-Hunter oversees all of DOHA's Administrative Judges, Department Counsel, Personnel Security Adjudicators, and administrative staff as either second or third level supervisor. Prior to his appointment to the Senior Executive Service as Director of DOHA, Mr. Russell-Hunter served as Deputy Director of DOHA, after serving for more than ten years as DOHA's Chief Department Counsel; during which time he was awarded the Secretary of Defense Medal for Exceptional Civilian Service in January of 2001. Mr. Russell-Hunter was appointed Chief Department Counsel in 1996, after serving as the Deputy Chief Department Counsel during 1995. Prior to becoming the Deputy Chief Department Counsel, Mr. Russell-Hunter served as a Department Counsel representing the Government in industrial security clearance due process cases. He is a frequent invited speaker on the topic of security clearance due process at national industrial contractor conferences convened by such groups as AIA/NDIA, the National Security Institute's "IMPACT" series, ASIS, and the CSSWG; as well as local chapters of the Industrial Security Awareness Council and National Classification Management Society. He regularly teaches the personnel security clearance process in courses at the DCSA's CDSE and the DC Bar. He has served on various working groups to reform the clearance process within the Department of Defense and across Government. He has served on the DoD/DNI Joint Security and Suitability Process Reform Team since its inception in June of 2007. He and the rest of the Joint Reform Team received the Director of National Intelligence's Meritorious Unit Citation in 2009. He was again awarded the Secretary of Defense Medal for Exceptional Civilian Service in January of 2017 for his leadership of DOHA and his interagency work on clearance reform.

Mr. Russell-Hunter is an Adjunct Professor of Law at the Georgetown University Law Center in Washington, D.C. where he teaches trial advocacy and civil litigation practice and where he was named the Charles Fahy Distinguished Adjunct Professor of Law for 2016-2017. Mr. Russell-Hunter is also on the faculty of the non-profit National Institute for Trial Advocacy program where he teaches trial advocacy and deposition skills to practicing attorneys and is the Director of the DC Deposition Skills Program and the Deposing the Expert Program. Mr. Russell-Hunter is also a Past President of, and a charter member of, the Federal American Inn of Court in Washington, D.C., where, from 1990 to 2010, he taught litigation and trial advocacy skills to practicing attorneys and law students. In the American Inns of Court, instruction by judges and practicing attorneys emphasizes ethics and civility in trial advocacy.

Prior to his nearly thirty years of federal service with the Department of Defense, Mr. Russell-Hunter practiced with the law firm of Pepper, Hamilton & Scheetz in Washington, D.C.

Mr. Russell-Hunter graduated *magna cum laude* from Syracuse University in Syracuse, New York, with a Bachelor of Arts degree with majors in both English and Political Science. While at Syracuse, Mr. Russell-Hunter was *Phi Beta Kappa* and received the Senior Leadership Award and the James F. Reynolds Award in Political Science. Mr. Russell-Hunter received his *Juris Doctor*, from Northwestern University School of Law in Chicago where he served on the school's Moot Court Board and practiced in the Legal Clinic.

Mr. Russell-Hunter is a member of both the Commonwealth of Pennsylvania and District of Columbia Bars. His direct office number is (703) 696-4751.