National Industrial Security Program Policy Advisory Committee (NISPPAC) Meeting
Wednesday, October 27, 2021 - 10:00 a.m. - 1:00 p.m.
National Archives and Records Administration (NARA)
Information Security Oversight Office (ISOO)
Meeting held virtually

Agenda

Welcome, Introductions, and Administrative Matters	**10 mins**
Action Item Follow Up	**10 mins**
Reports and Updates	
Industry Update	**15 mins**
Department of Defense (DoD) Update	**30 mins**
Defense Counterintelligence and Security Agency (DCSA) Update	**15 mins**
Office of the Director of National Intelligence (ODNI) Update Security Executive Agent	**10 mins**
Department of Homeland Security (DHS) Update	**5 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**
Working Group Update	**10 mins**
Defense Office of Hearings and Appeals (DOHA) Update	**5 mins**
Controlled Unclassified Information (CUI) Update	**10 mins**
General Discussion, Remarks and Adjournment	**10 mins**

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, currently known as the Defense Counterintelligence and Security Agency (DCSA). 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 the Associate Director for Operations & Industrial Security and Controlled Unclassified Information. 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 well as the Controlled Unclassified Information program per Executive Order 13556. Greg 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.

NISPPAC Government Biographies

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.

Dr. Jennifer Ann Obernier

Dr. Obernier joins the Department of the Navy as the Deputy Director for Security and Intelligence, Office of the Deputy Under Secretary of the Navy. In this role, she serves as the senior technical advisor for security and intelligence.

Prior to this assignment, Dr. Obernier spent 6 years with the Office of the Under Secretary of Defense for Intelligence (OUSD(I)). She joined OUSD(I) as a special operations policy analyst and held various positions, culminating as the Deputy Director of HUMINT and Sensitive Activities, providing oversight and advocacy for the Department's human-enabled sensitive activities and programs. In 2015, she was awarded the Secretary of Defense Medal for Exceptional Civilian Service.

Prior to joining OUSD(I) in 2013, Dr. Obernier was the Senior Intelligence Analyst for WMD-Terrorism at the Defense Intelligence Agency (DIA). During her six-year tenure at DIA, Dr. Obernier also deployed to Afghanistan in support of a Joint Interagency Task Force, conducting target development and supporting detainee and intelligence, surveillance, and reconnaissance (ISR) operations.

In 2006, Dr. Obernier became a program manager for bioterrorism detection R&D at the Department of Homeland Security. These programs procured forensic technologies and assays to support BIOWATCH, a bioterrorism detection system deployed in major US metropolitan areas.

In 2001, Dr. Obernier joined the National Academy of Sciences and became a Senior Project Director, managing committees of leading scientists to provide advice to Congress and the federal government on science and technology policy.

Dr. Obernier holds a Doctorate of Philosophy degree in Pharmacology from the University of North Carolina at Chapel Hill, where she was also a post-doctoral research fellow. She also has a Bachelor of Science degree in Molecular Biology from the Florida Institute of Technology.

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.

BIOGRAPHY

UNITED STATES AIR FORCE

JENNIFER M. AQUINAS

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

Prior to her current position, Ms. Aquinas served as the Division Chief, Security Policy and Oversight responsible for overseeing the development and implementation of Information, Personnel, and Industrial Security policy as well as Special Access Program policy. She has been instrumental in leading Air Force and Department of Defense efforts in personnel vetting and security reform.

Ms. Aquinas has more than 20 years of experience in security, working in a variety of assignments of increasing levels of responsibility. She entered civilian service in 2008 working for the Office of the Under Secretary of Defense for Intelligence. Thereafter, she joined SAF/AA where she led efforts to stand up an Air Force-wide Insider Threat program.

Ms. Aquinas served on active duty and in the Air Force Reserve between 1996–2016 as a Security Forces Officer.

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–present, Deputy 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 July 2020)

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

Ms. Heather M. Sims provides Security Strategy, Planning and Collaboration support to the Chief Security Officer at the General Dynamics Corporate Headquarters in Reston, Virginia. Her primary responsibility is to provide subject matter expertise for all security disciplines and insider threat guidance throughout the companies under the General Dyanmics (GD) umbrella.

Ms. Sims is also the current Industry Spokesperson to the National Industrial Security Program Policy Advisory Committee (NISPPAC). NISPPAC members avise 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 GD in September 2017, Mrs. Heather Sims was the Assistant Deputy Director for Industrial Security Field Operations at the Defense Security Service 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. 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 personnel security investigation mission back to the department for the federal government.

Prior to her current position 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 that were 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 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 O'Fallon, Illinois with her husband John Sims and their three children.

Rosael (*Rosie*) Borrero

Ms. Rosie Borrero is currently the Deputy Division Manager of Security for ENSCO, Inc. as well as the Senior Information Security Officer; responsible for managing, training and mentoring all corporate ISSM/ISSOs and providing all levels of security support for DoD and IC secure computing.

Rosie has over 20 years of experience in the cyber security field. She has held various information systems security-related 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 Masters 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.

Mr. David Tender is the Senior Vice President, ITPSO and Chief Security Officer for ASRC Federal. He has 35 years of experience not only in industrial security management but also 20 years of Air Force special security work as an active duty and active reserve member supporting our National Security.

As the Senior Vice President and CSO for ASRC Federal Mr. Tender is responsible for the entire enterprise security program as well as the Business Continuity and Emergency Management Program as well as the ASRC Federal Insider Threat Program. Mr. Tender is responsible for the Sensitive Compartmented Information (SCI) programs, the Department of Defense (DoD) programs as well as all the Special Access Programs (SAP). Mr. Tender is also matrixed in to the ASRC Federal senior leadership Risk Management Team and is a key member of the COVID leadership group. Mr. Tender is responsible to ensure that the security organization aligns with the stated objectives of security management of all the government compliance organizations, for policy requirements, training, facilities, and liaison with executive management support for the enterprise security organization.

Mr. Tender ensures in coordination with other ASRC leadership members that ASRC Federal is CMMC level three ready that the company's classified systems are inspection ready and that ASRC Federal facilities are protected and that the enterprise security program meets and practices the ASRC Federal ethical standards and code of conduct. Mr. Tender also ensures with leadership that ASRC Federal is meeting all its FOCI requirements. Mr. Tender's security organization are all active members in the different industry security organizations

Dave began his security career in 1984 when he enlisted in the United States Air Force until he left active duty in 1991 and joined the Air Force Reserve assigned to the Defense Intelligence Agency (DIA) until his retirement in 2009. Dave's industrial career started in 1992 as a part time FSO at SAIC and Dave worked his way up to the Deputy Director for Corporate Security at SAIC. Upon the SAIC split Dave was the Vice President of Security Operations at QinetiQ North America in 2010 which was merged into Vencore and then Perspecta where Dave was the Vice President and Chief Security Officer. Dave has had the honor of twice during his career having his organizations being awarded the DCSA Cogswell Award.

Dave is a long time member of National Classification Management Society (NCMS) as well as a member of the Industrial Security Working Group (ISWG), where he served as the chairperson for the ISWG PERSEC focus group and is now a member of the ISWG Board of Directors. Dave is also active with the National Defense Industrial Association (NDIA) as well as the numerous clearance reform tiger teams.

Dave is originally from Buffalo New York, and has lived in Manassas Virginia since 1991 and is married to Ginger Tender and have one Daughter Angela Tender

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.

Evan Coren, CUI Program Lead

Evan Coren is the Controlled Unclassified Information (CUI) Program Lead. With more than 19 years of experience in Federal government, including 7.5 years on the National Security Council staff and over 10 years on ISOO's staff, Evan's experience includes oversight of agency programs, interagency policy development and coordination, and helping agencies strengthen their programs.

With a Master's of Science from the London School of Economics in Comparative Politics with a focus on Comparative Constitutional Design, Evan looks at how humans, policies, procedures, training, and institutional design interact to produce specific outcomes.

Evan looks for opportunities to make policy user friendly and applied to achieve the desired policy goals.

Evan's outside of work passions including: hiking, camping, reading history books, traveling, theater (particularly anything funny and/or musicals), college basketball (Go Terps!), cooking and baking, and any chance to learn something new.

National Industrial Security Program Policy Advisory Committee (NISPPAC) Meeting Minutes October 27, 2021

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

Greg Pannoni 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 67th meeting on Wednesday, October 27, 2021 virtually. Mark Bradley, Director, information Security Oversight Office (ISOO), served as Chair.

Heather Sims, Industry Spokesperson, briefed on behalf of Industry. Heather thanked the outgoing NISPPAC members, Dan McGarvey and Dennis Arriaga for their service to the NISPPAC. Heather also welcomed the new members, Greg Sadler, and Dave Tender. She also called out Defense Counterintelligence Security Agency's (DCSA) improved collaborative efforts with Industry, which is appreciated, along with DCSA improving the personnel security mission over the last couple of years. She also called out the partnership with the Performance Accountability Council (PAC) Program Management Office (PMO) and key Industry members about Trusted Workforce (TW) 2.0.

Heather briefed there are some concerns with facility clearance/entity eligibility timeliness. NISPPAC Industry will be working with DCSA on the challenges they are coming across with the issues.

The risk management framework process continues to have inconsistencies throughout DCSA for approvals and being shut down, however, DCSA is working with Industry to hear their concerns and work through the issues.

There is a lot of work to do with the Defense Information Security System (DISS), but DSCA will be working with Industry on their concerns with the system and developing a more realistic implementation strategy.

Jeffrey Spinnanger, Director, Critical Technology Protection (CTP), Office of the Under Secretary of Defense for Intelligence & Security (OUSDI&S) requested the NISPPAC move to three meetings a year again. Heather Sims advised she would like to have more working groups.

He spoke about the new National Industrial Security Program Operating Manual (NISPOM) rule. Contractors had to comply starting August 24th. There will be an amendment to the rule to defer reporting and preapproval of foreign travel associated with SEAD 3 for contractors under Department of Defense (DoD) security cognizance until August of 2022. This amendment is to allow DCSA time to make adjustments to its IT system of record for receiving and processing from Industry of those foreign travel reports. DoD has canceled the DoD 5220.22-M NISPOM October 26, 2021. DoD's Washington Headquarters Services will update its issuance website, adding a note and link to the NISPOM federal rule in place of the DoD manual, so that people know that the NISPOM has not gone away. DoD is presently working on the second amendment to the rule to address the public comments received when the rule was first published back in December of last year. The second amendment will also go out for public comment to give those interested a chance to review and comment on resulting changes to the rule.

DoD sponsored a project with their university affiliated research center, Applied Research Laboratory for Intelligence and Security (ARLIS). ARLIS took on a pilot for cleared Industry's direct use of classified cloud services. Operating under the premise from the DoD cloud strategy, the cleared defense contractor supply chain needs to leverage and promote the use of cloud-based resources at all levels of classification, in order to create efficiencies across the enterprise, and to benefit from the power and security of collaborative and distributed computing. The adoption of cloud and eventual replacement of legacy classified systems is DoD should be thinking of in Industry. It will provide a measurable benefits with respect to oversight, security monitoring, and threat mitigation. Despite DoD's general recognition of the benefits of cloud use, no contractor has yet been successful in establishing a classified cloud system from a cloud service provider directly with a cleared contractor. To address this challenge, DoD asked ARLIS to leverage its own subject matter expertise, working with cloud service providers and substantial support from participating contractors. The Defense Information Systems Agency (DISA), DCSA, Office of the Chief Information Officer, and other government contracting activities observed several pilots that set out to demonstrate how a NISP contractor can, under current policy, leverage classified cloud services. ARLIS has developed a vendor neutral playbook describing a process to connect DISA and DCSA's current process guides, including wiring network connection process, security requirements guides, and security technical implementation guides, accreditation, and authorizations to operate architectural considerations. ARLIS has made a series of recommendations on requirements, authorities, process, and policy guidance and frame critical questions for legal interpretation to assist DoD in developing a repeatable process that allows for broad use of classified cloud by NISP contractors under DoD cognizance.

DCSA made DoD's Controlled Unclassified Information (CUI) training available in October 2020 via dodcui.mil. DoD components are in the process of implementing DoD policy requirements to safeguard CUI, and as a function of that, the requirements will flow down to the NISP through contract requirements. DoD will be working collaboratively with Office of the Director of National Intelligence (ODNI) on how the Intelligence Community (IC) undertakes to implement the CUI program, which ODNI is fine with doing.

DCSA will be required to expand its Foreign Ownership Control and Influence (FOCI) assessments to companies that do business with DoD via a contract or subcontract worth more than $5 million in accordance with section 847 of the fiscal year (FY) 2020 National Defense Authorization Act (NDAA). It requires a FOCI assessment and mitigation of risk of covered contractors doing business with DoD. The draft DoD instruction provides procedures for DoD to implement this requirement and is currently in coordination. Once the instruction is promulgated, the Office of the Undersecretary of Defense for Acquisition and Sustainment will develop and publish a DFARS clause in collaboration with OUSDI&S and DCSA addressing section 847 requirements.

There is a provision in section 1629 of the FY 2020 NDAA that states if both entities that form a joint venture (JV) are cleared, the JV company itself does not need an Entity Eligibility Determination (EED)/facility clearance (FCL). There is also similar language in a Small Business Administration (SBA) federal rule published late last year. DoD is updating DoD internal policy to reflect the legislation and address the conflicts it poses with current NISP policy. Jennifer Aquinas, United States Air Force (USAF), briefed on challenges surrounding solicitations for classified contracts. The USAF recently released a solicitation for a classified contract and one of the bidders was an unpopulated joint venture whose member companies hold facility clearances at the level of contract performance. In accordance with NISP policy requirements, USAF indicated a need for the JV itself to be cleared in order to access

classified information, but due to the NDAA language, the JV protested, and the Government Accountability Office (GAO) sustained the protest in favor of the JV. In other words, the GAO stated that since both members are of the joint venture are cleared, requiring the JV to hold its own facility clearance is inconsistent with statutory and regulatory provisions. The Air Force needs to comply with the NDAA until the policy and regulatory issues are resolved since it directly conflicts with the NISP requirements. The SBA rule appears to eliminate the requirement for a JV to have an EED/FCL if the entities making up the joint venture already have EEDs themselves, however, this interpretation of the regulation's language is not actually what the regulation intends, and it contradicts NISP requirements. ISOO will be issuing an ISOO notice.

Mr. Keith Minard, Senior Policy Advisor, Critical Technology Protection, DCSA, briefed next. Related to the NISPOM rule, DCSA established a web page to provide a central source of information. They also created the Get Ready for the Rule video, which provided cleared Industry with a brief overview of what to expect and how to prepare for the NISPOM rule. They also provided a cross-reference tool that allowed those familiar with the DoD NISPOM to more easily find similar portions in the NISPOM rule. The tool has been revised to address some minor changes and reposted on the CDSE website. There were seven NISPOM rule related webinars. The senior management official (SMO) webinar had many SMOs in attendance, which served to advise SMOs of their responsibilities. It was recorded and is available on the NISPOM rule webpage. DCSA created three audio shorts and accompanying slides for communicating specific NISPOM requirements. The topics included SMO responsibilities, a short overview of the rule, and an Underwriter's Laboratory (UL) 2050 Intrusion Detection System (IDS) certification changes.

DCSA is updating their FAQs on SEAD 3 and the recorded webinar on SEAD 3 is posted on their webpage. They also created a desktop tool to help Industry better find the sections of the Industrial Security Letters (ISLs), the tables, and also the reportable sections of the SEAD 3 itself to better enable reporting activities. It serves as a quick reference guide and can be kept on your desktop. While the NISP is newly implementing the SEAD 3 requirements, they asked that ODNI talk about challenges, best practices, and outcomes of SEAD 3 implementation in the federal executive branch at the next NISPPAC, so that everyone can use lessons learned as we move forward for those things. DCSA will not begin oversight of SEAD 3 requirements in our assessments until March 1st, 2022.

DCSA's website has a posting on the new security review model. It became effective September 1st. DCSA is following that model now in the conduct of reviews.

DCSA will be onboarding Industry over the course of FY 2022 in National Background Investigation Services (NBIS). The DCSA website is being updated with additional NBIS information to keep Industry informed.

Sara Coonin, DCSA, briefed on DCSA's regional realignment of its field operations effective October 1, 2021. The new structure merges the existing field mission areas into a consistent four region structure that includes Western, Central, Eastern and Mid-Atlantic regions. The changes will not change the mission requirements and business practices. The only real impact for stakeholders involve some point of contact updates. If a DCSA point of contact was changed for a cleared contractor, your relevant Industrial Security Representative (ISR), Counterintelligence Special Agent (CISA) or Information Systems Security Professional (ISSP), should have contacted you to facilitate a seamless transition to your new point of contact. Only about 5% of DCSA's cleared contractor facilities experienced a change in their

field office as a result of this realignment. There is no change to overseas operations. You can find the updated regional structure alignment on DCSA's website.

Ms. Valerie Kerben, Chief, Policy & Collaboration Group, Special Security Directorate, National Counterintelligence and Security Center (NCSC), ODNI, briefed next. Ms. Kerben provided updates on changes to NCSC's organizational structure, including that the Scattered Castles program and continuous evaluation system, have been moved to a new directorate called the Mission Capabilities Directorate for more focus and efficiency. Additionally, the National Insider Threat Task Force is now in a new directorate called the Enterprise Threat Mitigation Directorate.

Ms. Kerben also provided updates on TW 2.0. ODNI, along with the Office of Personnel Management (OPM) and the Suitability, Security, and Credentialing, PAC PMO, is tracking agency implementation of TW 2.0 milestones. The January 15th, 2021 Joint Executive Agent Correspondence explained the shift into Phase Two of TW 2.0, which includes policy development and implementation for the new government wide approach. The January 2021 memo further explains the phased implementation strategy for Phase Two, and outlines the requirements for transitional states (TW 1.25 and TW 1.5). The ultimate goal of transitioning is to get the national security population into a continuous vetting (CV) capability, which will satisfy traditional periodic reinvestigation requirements. As of September 30, 2021, agencies should have enrolled their full national security population in at least a TW 1.25 capability. On September 30, 2022, agencies must enroll their full national security population in a TW 1.5 capability.

Ms. Kerben also shared that the Federal Personnel Vetting Guidelines are currently in coordination with ODNI and OPM (the Security and Suitability/Credentialing Executive Agents) for signature and issuance. These Guidelines provide the outcomes associated with investigations, adjudications, and personnel vetting management activities. These Guidelines align with the Federal Vetting Core Doctrine, which was put into the Federal Register in February 2021 and provides the overarching philosophy and the guiding principles for personnel vetting.

The Federal Personnel Vetting Investigative Standards are going through coordination for signature and issuance. These Standards realign the five tiers of investigations into three tiers. The PAC is also working on an implementation strategy, so agencies will understand what they need to do to prepare for TW 2.0. The Strategy identifies key milestones.

ODNI referred members to the recently released statement regarding COVID-19 and how mental health stressors should not impact national security eligibility and determinations. Counseling and undergoing treatment as a result of COVID, or the associated stressors, should not in itself be considered negative or disqualifying when rendering an eligibility or access determination.

Rich DeJausserand, Deputy Director for Industrial Security, briefed for Department of Homeland Security (DHS). DHS continues to work with DCSA and their personnel security team on implementation of the NISPOM rule.

Mark Hojnacke, Director, Office of Security briefed for the Department of Energy (DOE). The DOE Acquisition Rule (DEAR) established their policies and procedures for implementing and supplementing the Federal Acquisition Rule (FAR) and the DEAR requires compliance with DOE safeguard and security directives rather than referencing compliance within NISPOM. DOE implements the NISPOM through a series of departmental security directives, including INFOSEC, personnel security, physical security,

safeguard and security planning, and their protective forces. This arrangement allows DOE to establish security requirements for all of the assets within the department, particularly, where in addition to classified materials, our special nuclear materials that are under our control. While the NISPOM rule was being developed, DOE conducted a review of all of relevant security directives to identify any gaps that would need to be addressed. This review identified that the SEAD 3 language needed to be included in their directive, specifically the requirements for reporting and training. The SEAD 3 requirements will be included in their personnel security directive, which are currently under revision.

Dennis Brady, Chief of the Security Management and Operations Branch, gave the Nuclear Regulatory Commission's (NRC) update. For SEAD 3, the NRC has implemented all reporting requirements for Security Executive Agent Directive 3, with the exception of personal foreign travel approval. The agency has a foreign travel approval tool in development and has plans to launch the tool in mid-January of 2022. The NRC's industrial security program continues to be fully implemented.

A spokesperson gave the Central Intelligence Agency's (CIA) update. Regarding the status of the agency in NISPOM compliance, the changes will be rolled out shortly. They are in the process of engaging with Industry and will be highlighting future Industry events, such as conferences, and workshops. Regarding SEAD 3 reporting requirements, they already have reporting requirements in place. The information reported to the company's security officer is forwarded to the CIA. They review those on a case by case basis.

Greg Pannoni, ISOO, briefed next on the clearance working group. He advised that NISP entity cost collections discussions are ongoing. It is part of an overall reform effort within ISOO. ISOO embarked on a reform initiative to simplify the cost collection and other data requirements to try and improve upon the data that we collect as it relates to things such as self-inspection reporting data, classification activity type data, etc. The executive orders for both the NISP and for the classified program, as well as the two applicable directives to those two orders, mention a requirement for cost collection. A number of meetings have been held with DoD as the Executive Agent, to come up with a consensus position about the costs that are required on behalf of contractors to implement the requirements of the NISP. We will then reconvene with the other CSAs, then we will bring NISPPAC Industry in for input before finally advising the NISPPAC chair on the way forward for collecting these data relative to cost in this case that are incurred for implementing the requirements of the NISP by contractors. During the clearance working group, UL briefed updates that they are working on for the UL 2050 standard intrusion detection standard for supplemental controls for safeguarding classified.

David Scott, DCSA, briefed on DCSA's information systems update with slides. For FY 2021, they have seen an uptick in registered systems and on Enterprise Mission Assurance Support Service (eMASS) users. They are going to have eMASS give an automatic record that is 180 days, 90 days, 60 days, etc., to the contractor Information Systems Security Manager (ISSM) when systems expire. They are also going to take a look at closing out a lot of disestablished systems that are coming in and closing that on that cycle.

From a Command Cyber Readiness Inspection (CCRI) perspective, they have deferred all of those CCRIs over the course of the last 18 months. Their certified CCRI reviewers are going virtual training in preparation for DCSA going on site and conducting CCRIs.

The triage process is where contractor staff review the packages when they first come in from Industry, making sure that the ISSPs receive a complete package for their initial risk assessment. There still are

some significant issues missing artifacts and the test results, but have seen an improvement over the past six months.

They are also trying to implement a package workflow enhancement within eMASS. Industry and the ISSM will see exactly where their package is. The ISSM would have their own role within a package workflow.

They are also looking to provide additional job aids. They are going to provide additional guidance on security classification, and how to address that using eMASS, which will be shared with the NISA working group prior to publishing.

The DCSA Assessment and Authorization Process Manual (DAAPM) 3.0 is going through an update, and is in the initial stages. They will be partnering with the NISA working group.

The NISP connection process guide is near completion. The NISA working group should receive it for their comments soon. It is a how to guide for Industry and their government stakeholders if they have contractual requirements to interconnect within the NISP.

There is still currently a pause on new Enterprise Wide Area Networks (eWANs), as they are still looking to provide additional clarity for this program. They have six current operating eWANs. We had a NISP eWANs participant meeting.

Heather Green, DCSA, briefed their personnel vetting update. Slides were provided.

Tracy Kindle, DOE, briefed their metrics. Slides were provided.

Chris Heilig, NRC, briefed their metrics. Slides were provided.

Perry Russell-Hunter, Director, Defense Office of Hearings & Appeals (DOHA), provided DOHA's update. He first recognized Valerie Heil for representing the very best of expert professionalism in Industrial Security and Government over many years of exemplary service. DOHA continues to make maximum use of telework except for the personnel who are conducting and supporting the in-person administrative hearings, the DOHA Administrative Judges, Department Council and support personnel. Statements of Reasons (SORs) are still going out in typical numbers and are timely. They currently just over 330 SOR reviews pending, which is a typical number. DOHA reviewed 1,200 SORs during the first four months of calendar year (CY) 2021. From May to August, DOHA reviewed 802 draft SORs. Year to date, over 2,000 draft SORs have been reviewed, averaging about 225 per month. At this pace, DOHA is on track to review about 2,700 SORs for CY 2021. Between 2017 and 2019, DOHA reviewed a typical average of 2,600 SORs per year. In FY 2021, DOHA legal reviewed and revised 3,021 SORs.

There has been discussion in past meetings of DOHA providing SORs directly to Industry and tracking them, but the MOA required to do this has been delayed by a number of external factors. I do not currently have a timeline for when this will be taking place.

The pandemic impacted the hearing process because DOHA was having challenges with conventional video teleconferencing due to the simple fact that there would often be no operators available at the other end of the line at the location where DOHA needed to reach, DOHA had tested and made good

and effective use of something called the Defense Communications System (DCS) to conduct remote online virtual hearings for clearance holders and clearance applicants in locations where travel would still be unsafe or where we could not reach the individual using conventional video teleconference technology. With the sunset of DCS, DOHA will be holding hearings using Microsoft Teams 365 in FY 2022. DOHA has also continued to hold in-person hearings throughout the pandemic whenever and wherever possible and will continue to do so.

Evan Coren, Implementation Lead for CUI, ISOO, briefed on ongoing CUI efforts. When the CUI FAR clause comes out, ISOO will host a Question and Answer session to get any questions answered before submitting comments. ISOO has also been working with Microsoft regarding Microsoft 365. Their sensitivity labels for security sensitivity has been an issue when trying to do metadata regarding CUI. They are working on the issue. Personnel should type on the document the banner markings that are required, and if they're only dealing with CUI basic, have a tag for CUI basic versus trying to create a tag for every category.

In addition to CUI working groups, ISOO has also have been working with the National Insider Threat Task Force. There will be a joint issuance with them on the intersection between insider threat and CUI.

Everyone is encouraged to take CUI markings training being offered by ISOO, which is announced at https://isoo.blogs.archives.gov/. There are also training resources at https://www.archives.gov/cui/training.html.

The NRC has been working on an information sharing agreement structure that would allow multiple federal agencies to sign the same information sharing agreement with third party partners of Industry or academia to allow more common, less complicated ways to share information.

Valerie Heil, OUSDI&S, briefed next. She advised that there was a question about the applicability of section 847 of the NDAA. It is also section 847 of Public Law, 116-92. The legislation is specific to DoD. When DoD establishes this effort through a policy issuance, and then a subsequent DFAR case, it will be outside the NISP.

Most speakers congratulated Valerie Heil, Associate Director, Industrial Security for the OOUSDI&S; Counterintelligence, Law Enforcement & Security.

The next NISPPAC is scheduled for April 27, 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

None.

Questions and Answers from the NISPPAC

Q. At the last NISPPAC, there had been discussion about the Solid State Drive (SSD) sanitization issue. Since then multiple vendors have announced they will no longer product hard drives that are not SSD based. What can be done?

A. At this time, the National Security Agency (NSA) has not cleared any other sanitization method, so there are no other options at this time.

Q. The SEAD-3 ISL 2021-21 speaks to foreign travel and certain destinations that require DCSA CISA interviews prior to travel. Are we communicating these changes and requirements across the security team (Government and Industry)?

A. Yes. The ISL addressing SEAD 3 reporting requirements provides guidance specific to NISP contractors under DoD security cognizance. The requirement to obtain a DCSA CISA briefing prior to travel applies only to those NISP contractors under DoD security cognizance.

Q: Is there a plan to become more transparent with the status of favorable or unfavorable fingerprints for industry? We have found that our government security command officers are able to see more detail on subject's fingerprints being favorable or unfavorable which affects the issuance of CAC/PIV cards. Presently DISS does not provide that level of detail for Industry. Would this be something that can be reflected in SWFT or NBIS with its future rollout?

A. The fingerprint results are not provided to Industry as that would be a violation of the Privacy Act, similar to not sharing the results of an investigation or if a case is in due process, etc.

Q. Joint ventures were mentioned due to an issue with a joint venture bidding on an Air Force project. They talked about a conflict with the NISP requirements and NDAA and SBA. What is the NDAA?

A. There are two separate requirements effecting JVs that is the SBA rule and Public Law 116-92, Section 1629, National Defense Authorization Act for FY 2020.

Q. Reference CV enrollment: How accurate is the statement that all cleared individuals have been enrolled in CV? A significant number of industry personnel are not yet enrolled in CE.

A. Departments and agencies are transitioning to conducting CV as part of the TW 2.0 initiative. Departments and agencies enrolled most of their national security population in at least TW 1.25 and moving towards enrolling all national security populations TW 1.5 capability. Once in TW 1.5, departments and agencies can cease conducting traditional periodic reinvestigations for individuals enrolled in continuous vetting. Departments and agencies must enroll their entire national security population into TW 1.5 by September 30, 2022.

NISPPAC Attendance

Abbott, Aprille
Abbott, Gabriele
Abrams, Nikki
Ackerman, Daniel
Adams, Kendall
Aden, Casey
Adissu, Mekdes
Agustin, Ben
Akers, Lynetta
Albalos, Raven
Alexander, Christine
Alexander, Treva
Allen, Nicole
Amaya, Isabel
Andablo, Yvette
Andrade, John
Andrews, John
Anello, Tonya
Aquinas, Jennifer
Arbuckle, Leslie
Armstrong, Robert
Arnold, Diana
Arriaga, Dennis
Ashley, Janet
Auldridge, Kelly
Avila, Donna
Backhus, Annie
Bailey, Lynn
Bailey, Zaakia
Barbee, Lisa
Barnhart, Jason
Bastien, Addie
Battiston, Matthew
Baugher, Kimberly
Bauriedl, Sigmund
Baxter, Jordan
Beasley, Michelle
Belcher, Lara
Bellagamba, Barbara
Bemah, Kimberly
Bensie, Evelyn
Berhalter, Teresa
Berry, Kathleen
Bethea, Nasu
Bhalla, Ginny
Bibee, Rachel
Biggers, David
Biggs, Sarhonda
Bland, Booker
Blount, Richard
Boaston, Thomas
Boccalino, Michael
Bock, Kristy
Bodrick, Detra
Bolick, Gregory
Boling, Daniel
Bongiorno, Nick
Borland, Jennifer
Borrero, Rosie
Bosch, Lucas
Bosket, Jeff
BoulwareColeman, Chelsi
Bowman, Jennifer
Bradley, Mark
Brady, Denis
Brain, Steven
Brandt, Elizabeth
Brandt, Richard
Braxton, Kishla
BrennanFontes, Jean
Broadie, Connie
Broglin-Bartlett, Darinda
Brokenik, Patricia
Brokenik, Trish
Brooks, Beverly
Brooks, Valerie
Broussard, Derrick
Brown, Shirley
Bruce, Erin
Bruder, Bethany
Brumfield, Lisa
Bruzzese, Tracy
Burger, Bridget
Burgos, Sasha
Burns, Lynn
Burrell, Lisa
Burrough, Tonia
Busch, Melissa
Bynum, Mark
Byrge, David
Call, Samantha
Callier, Jewel
Calloway, Victor
Capsalis, Corey
Carbone, Anthony
Cardella, Thomas
Carlyon, Michelle
Carney, Jacqueline
Carson, Teresa L.
Castel, Jason
Caudle, Robert
Cavano, Jeffrey
Champion, Mariellen
Chappell, Curtis
Charyton, Dianne
Chaumont, Luis
Chavez, Steven
Cherry, Florence
Chiocchio, Gina
Chituras, Jimmie
Christen, A. Bryan
Christian, Heather
Christian, Laurie
Church, Taylor
Cinelli, Giovanna
Cippel, Melissa
Clader, Heather
Clapp, Julie
Clark, J. G.
Clark, Larry
Clarke, Dan
Clarke, Louis
Clasen, Melissa
Cline, Nathan
Coburn, Catherine
Coleman, Johnathan
Coleman, Yvette
Collins, Randi
Collo, Robin
Colon, Kim
ConawayManson, Byron
Condon, Jessica
Condon, Jessica
Conlon, Denise
Connelly, Michael
Conquest, Karlyon
Cook, Krista
Cooke, David
Coonin, Sara
Cooper, Nicole

Coppel, Drew
Coren, Evan
Corsey, Michael
Cottrell, Christopher
Crabtree, Misty
Craig, Diane
Crew, Kimberly
Crickenberger, Joy
Cronin, Scott
Croson, Matthew
Cullison, Ashley
Daniel, Cindy
Daniels, Jordan
DAnthony, Stacey
Davis, Estelle
Davis, James
Davis, Mark
Davis, Michael
Davis, Sarnsuray
Dawson, Michelle
Dawson, Steven
Deabler, Angela
Dean, Kelsey
Dean, Mary
Dejausserand, Richard
Delacruz, Pauldelan
Deloney, Ryan
Demers, Michael
Denegal, Robert
Dent, Lillian
DeTurk, Eric
Diggs, Brenda
Dinkel, Jane
Dinkel, Jane
DiSante, Pete
Dixon, Jennifer
Dixon, Kenya
Doherty, Ed
Dorian, Jenna
Dotson, Virgil
Doubleday, Justin
Dougherty, Patrick
Douglas, Susan
Doyle, Sean
Driscoll, Michael
Dubay, Greg
Duke, Christina
Dukoff, David
Dunn, Andrea
Durkin, Tracy
Dyson, India
Eckel, Mark
Eckert, Ed
Eckmeder, Carol
Eddins, Kristina
Eddy, Jo Ann
Edmonds, Tracy
Egan, Amanda
Engholm, Kristy
England, Michael
Enriquez, Marcus
Epps, Danette
Equels, James
Ervin, Christopher
Ervin, Vicki
Escobedo, Robert
Essex, David
Exile, Samuel
Fabozzi, Madeline
Faller, Mike
Farmer, Anne
Fehlner, Scott
Fidler, Elizabeth
Finklea, Anthony
Fisher, Darci
Fisher, David
Flaherty, Joann Emma
Forrest, Chris
Forsgren, Branden
Franklin, Jennifer
Frederick, Kelly
Freeman, Lisa
Funicello, Kasey
Funicello, Lorena
Futrell, Joshua
G., F.
Gabeler, Jennifer
Gardner, Kelly
Garvin, Kelly
Gatlin, Ramona
Geisler, Angela
Gibbs, Diane
Gibbs, Katrina
Gibson, Sharon
Ginder, Linda
Glassic, Scott
Gleason, Kimberly
Godbold, Debbie
Godfrey, Shaneequa
Goldstein, Donald
Gomez, McShane
Gomez, Nellie
Gonchar, Cole
Graham, Jennifer
Graham, Melissa
Grandfield, Richard
Gray, Juaquita
Gray, Tonya
Greaver, Angie
Green, Heather
Gregory, Vanessa
Griffiths, Hasina
Grimes, Daniel
Grinnell, Matthew
Gulack, Jeff
Haire, Tamara
Halloran, Jennifer
Hamilton, Jill
Hamilton, Pamela
Hamilton, Pamela
Harris Pagán, Heather
Harris, James
Harris, Melvese
Harris, Tamara
Harvey, Dawn
Hawk, Jason
Heaton, Pamela
Heavner, Alyssa
Heil, Valerie
Heilig, Chris
Helstowski, Emily
Henderson, Kaila
Henry, Steven
Hensley, Michael
Herbst, Jonathan
Hernandez, Niel
Hertzog, Conrad
Hidle, Tamara
Higgins, Heather
Hill, Brett
Hill, Jessika
Hisey, Jackie
Hodge, Marie
Hodges, Hope

Hogan, Teresa
Hojnacke, Mark
Hollandsworth, Matthew
Hoover, Ronald
Howard, Heather
Howard, Justin
Howell, Adrianna
Howell, Mark
Huber, Donna
Hulet, Michael
Hurley, Tim
Hurst, Richard
Husker, Frank
Hutcheson, Amy
Hutchison, Alicia
Hynes, Timothy
Illidge, Kaitlin
Ivey, Julie
Jackson, Sonja
Jackson, Stephen
Jackson-Marquard, Kirsten
Jacobs, Kendra
Jensen, Kathryn
Jett, Christina
Jiggetts, Lauren
Johns, Adriane
Johnson, Troy
Johnson, Tyler
Jones, Cecilia
Jones, Derek
Jones, Kenneth
Jones, P.
Jones, Tara
Jongema, Linwood
Jordan, Ryan
Jordan, Yvonne
Kaiser, Michele
Kalman, Eric
Kamilova, Kamilya
Kaohi, Cathe
Kaohi, Catherine
Kay, Susan
Kennedy, Beverlee
Kerben, Valerie
Kerr, Julie
Kindle, Tracy
King, Anthony
King, Christyne
Kirby, Jen
Kitts, Karen
Klaczyk, Joseph
Klag, Toni
Klink, Carolina
Knarr, Matthew
Kozacek, Shelly
Kraus, Joseph
Kresge, James
Krug, Richard
Kyzer, Lindy
LaBeach, Stephanie
Lai, Kuan
Lambert, Brett
Lankford, Cheree
Lauer, Tammie
Lawhorn, Jeffrey
Lawley, Sean
Lawrence, LeVar
Lawrence, Mitch
Lawson, Pamela
Laxa, John
Laybourne, Krista
Leach, Vannessa
Leadbeater, Holly
Lee, Jennifer
Lee, Jessica
Leiter, Tammy
Lettera, Brenda
Lewis, Natasha
Lightner, Carol
Limon, Katherine
Liner, Marquiz
Lopez, Robert
Lord, Ginger
Lorenz, Lori
Lotwin, Andrew
Love, Kristen
Lucock, Cynthia
Ludwig, Clifford
Luera, Xanne
Lundquist, Margaret
Ly, Dan
Ly, Daniel
Mace, Bernadette
Macey, Christopher
Malbone, Nicole
Malloy, Barbara
Manglona, James
Manning, Lesa
Mantooth, Mark
Maples, Lauren
Marks, Michael
Martens, Sheri
Martinez, Cesar
Martino, Gail
Massaro, James
Mayberry, Grant
Mayercin, Elizabeth
McCarthy, Leslie
McClanahan, Cheri
McCloud, Adrienne
McConkey, Susan
McDaniel, Douglas
McGarvey, Daniel
McKay, Jennifer
McLaughlin, SJ
McLeod, Donna
McLeod, Risa
McLin, Anna
McManus, Daniel
McMillian, Toni
Mcnichol, Lindsey
McNichol, Lindsey
McRae, Robert
Measures, Lisa
Mechem, Stormie
Medina, Servio
Medina-Creel, Tina
Mencin, Brett
Merritt, Marcus
Metcalf, Jessica
Meyer, T
Mignogna, Christal
Miller, Dean
Miller, Lisa
Miller, Mark
Miller, Robert
Miller, Susan
Minard, Keith
Minard, Verna
Mingl, Sherry
Mitchell, Bruce
Mitchell, Janice
Mitchell, Melody
Mittleman, Elaine

Moon, Epiphany
Moore, April
Moore, Shalonte
Morales, Alana
Morrill, David
Morrison, Robert
Moseley, Paula
Mosier, Jennifer
Moss, Leonard
Motelet, Michelle
Mullins, Paula
Murdock, Camellia
Myers, Allison
Nane, Amy
Neale, Cynthia
Needle, Kandace
Nesmith, Kamilah
Ngo-Ho, Shirley
Nickel, Robin
Nix, Chad
Noad, Alfonso
Noles, Chad
Norman, Diane
Norton, Paul
Nunley, Anne
Nunn, SeKitha
Nunnenkamp, Kenneth
O'Brien, Michael
O'Kane, Elizabeth
Obernier, Jennifer
Omiatek, Mary
Oppenhagen, Christine
Orellana, Tania
O'Rourke, Frances
Ososkie, Charles
Pahl, Kayla
Palmar, Jose
Pannoni, Greg
Pappas, Joyce
Parker, Andrew
Parmenter, Debra
Parr, Doris
Paxton, Larry
Pekrul, Mark
Penharlow, Karen
Persinger, Jon
Pettengill, Chantel
Phagura, Satminder
Phalen, Charles
Pherson, Kathy
Phillips, Earl
Pinkney, Shanna
Porter, Lizet
Potts, Nichole
Powell, Johnny
Power, Kyla
Price, Emmett
Provencher, Marguerite
Pulliam, Donna
Pyles, Larry
Qualley, Linda
Quattrone, Anthony
Quinones, Francheska
Ragland, April
Raju, Clara
Ramaswamy, Shobha
Rarig, Karl
Ray, Richard
Reardon, Amy
Reff, Royal
Reid, Jennifer
Reinicke, Toni
Renzella, Allyson
Revy, Lisa
Rhamy, Alicia
Ricci, Cheryl
Rickell, Cathy
Riggins, Rebecca
Robinson, Sherry
Roche, Matthew
Rodrigues, Luciana
Rodriguez, Chamagne
Rogers, Geraldine
Rogers, Geraldine
Ross, Stephanie
Rossiter, Lisa
Roswal, Andrew
Royster, Cameron
Rubiano, Robert
Rucker, Latrice
Russell, Thomas
Russell-Hunter, Perry
Rust, Dan
Sabre, Lisa
Sadler, Greg
Saenz, John
Sanchez, Elizabeth
Sanchez, Sunni
Saurer, Phillip
Savage, Andrea
Schellhase, August
Schindler, Brittany
Schneider, Sandra
Schneider, William
Schools, Patricia
Schymanski, Catherine
Scott, David
Scott, Yvette
Sease, James
Seiler, Jason
Senutovitch, Diane
Sergent, Matthew
Settles, Christina
Shackelford, Sheri
Shaw, Cheyenne
Shaw, Melissa
Shimamura, Judy
Shular, Jacqueline
Simm, Graham
Simpson, Kimberly
Sims, Heather
Sims, Taniesha
Singer, Zaree
Singletary, Patrice
Sivak, Tracy
Sjodahl, Debbie
Skinner, John
Smith, Anthony
Smith, Janice
Smith, Linwood
Smith, Susanne
Smith, Tracey
Smith, Victoria
Soltis, Sheldon
Sotelo, Michael
Speace, Garrett
Speier, Brent
Spilman, Pamela
Spinnanger, Jeffrey
Spivey, Debra
Stehlik, Terry
Steinke, Sue
Steinour, Jason
Stephens, Brooke

Stephens, Tod
Steudlein, Steven
Stevenson, Regina
Stewart, Michael
Stolkey, Christopher
Stone, Cheryl
Stratton, Ana-Jeanne
Sumpter, Valerie
Sutphin, Joanna
Swann, Charisse
Switala, Jamie
Sylvester, Steven
Taft, Dianne
Talley, Thomas
Tarpley, Laura
Tate, Brenda
Tate, Charles
Taylor, Chalyndria
Taylor, Michelle
Taylor, Troy
Teemley, Kate
Teets, Amy
Terrell, Shatonna
Theriault, Jason
Thibault, Crystal
Thibodeaux, Kristie
Thomas, Douglas
Thomas, Jeannie
Thomas, Nina
Thompson, BLinda
Thompson, Courtney
Thompson, Donna
Thompson, Kathy
Thornton, Diana
Thornton, Samantha
Tiffee, Bradley
Tillson, Aric
Timmons, Katie
Timmons, Katie
Tipton, Paula
Todd, Joseph
Toney, Carolyn
Tran, Anh
Tringali, Robert
Tsukamoto, Krystina
Tucker, Joni
Turner, LaTonya
Turner, Shawntelle
Ty, Emmanuel
Ulery, James
Vaccariello, Jeffrey
Vachon, Jackie
Vander Ven, John
Vaughan, Tom
Vaughn, Susie
Vish, Jeff
Volak, Martha
Waddle, Jill
Wade, Tracy
Wallace, Charlene
Ward, Amanda
Ware, Laura
Warner, Jean
Warzecha, Marisa
Washington, Harold
Washington, Keshia
Watters, Michelle
Weatherby, Bradley
Webber, JoAnn
Weber, Kathleen
Webster, Morgan
Weeks, Jeannine
Weikel, Tara
Wells, Matthew
Wendell, Jeremy
Werner, Roxann
Wesemann, Jodie
Wever, Xiomara
Whatley, Beth
White, Iryna
White, Maria
Whitehead, Lynette
Whitley, Stephanie
Whittaker, Ralph
Williams, Kristin
Williams, Stacey
Williams, Syreeta
Wilson, Francoise
Wilson, John
Wilson, Melissa
Winford, Donneaka
Winkelman, Mark
Winn, Terrance
Winton, Tracy
Wisnosky, Roger
Woldridge, Marya
Wood, Delvin
Wood, Lemy
Woodall, Christopher
Woodard, Teresa
Woolf, Michael
Worsham, Robert
Wright, Eunice
Wright, Paula
Wright, Tracy
Yenigun, Katie
Yeow, Kim
Young, Roxana
Yuhas, Rae
Yurechko, Victoria
Zalovick, Brittany
Zimmerman, Patricia
Zweil, Alison

FIELD TRANSFORMATION

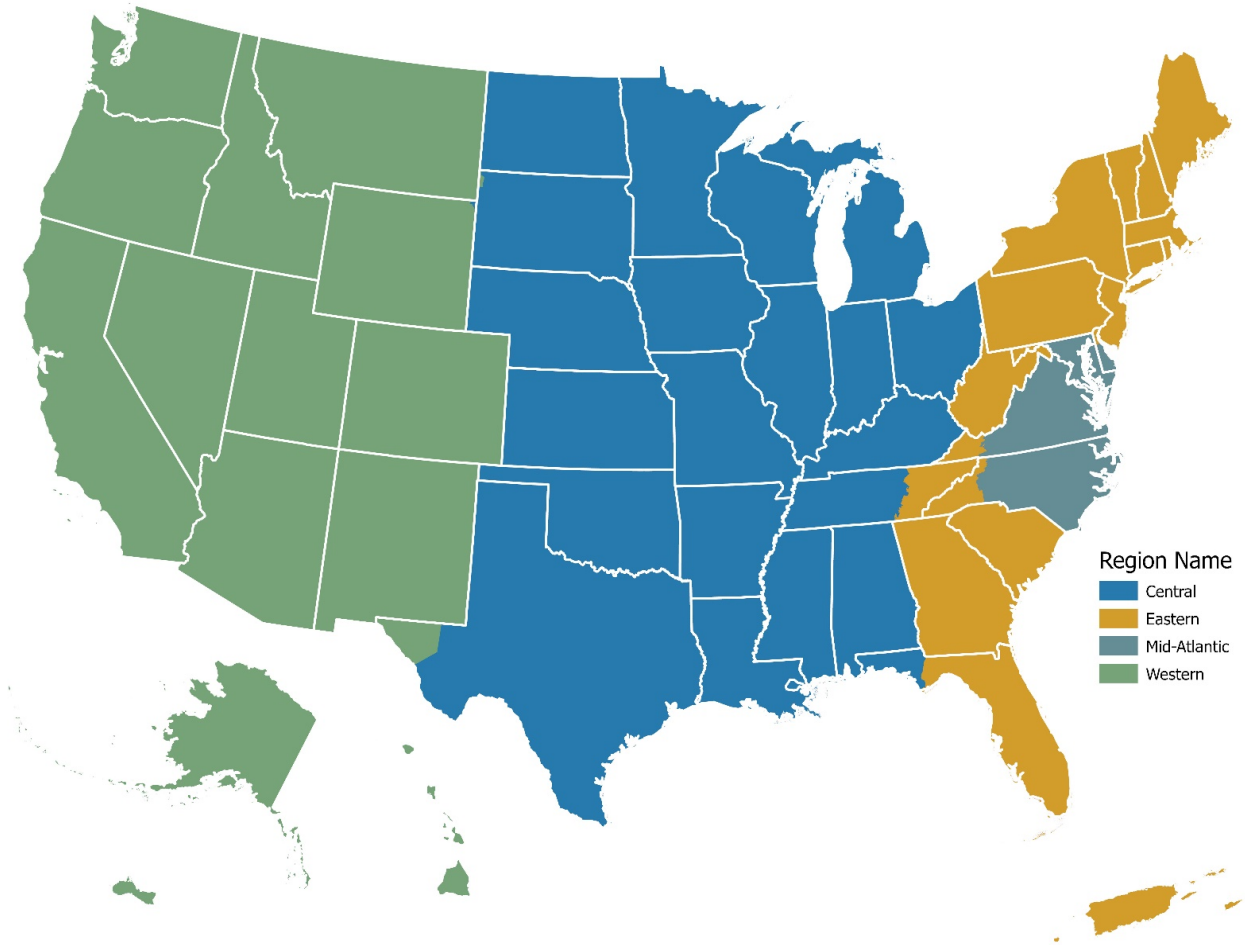
NISPPAC Briefing

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

October 2021

New DCSA Field Structure

DCSA established a new regional field structure on October 1, 2021 that merges existing field mission areas into a consistent four-region structure.



Integrating DCSA's Field

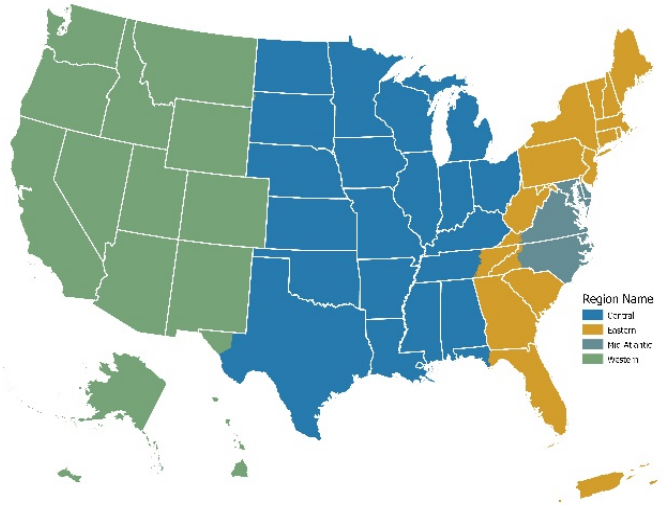
IMPACTS TO CUSTOMERS

For some stakeholders, DCSA points of contact may change. CISAs/ISRs/ISSPs are making these notifications as needed.

The updated regional structure will not impact the quality of service provided to customers:

- No change to the mission
- No change to requirements
- No change to standard DCSA business practices

The New Structure



DCSA
NISA WORKING GROUP
UPDATE

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

DAVID SCOTT
NISP AUTHORIZATION OFFICE
CRITICAL TECHNOLOGY PROTECTION

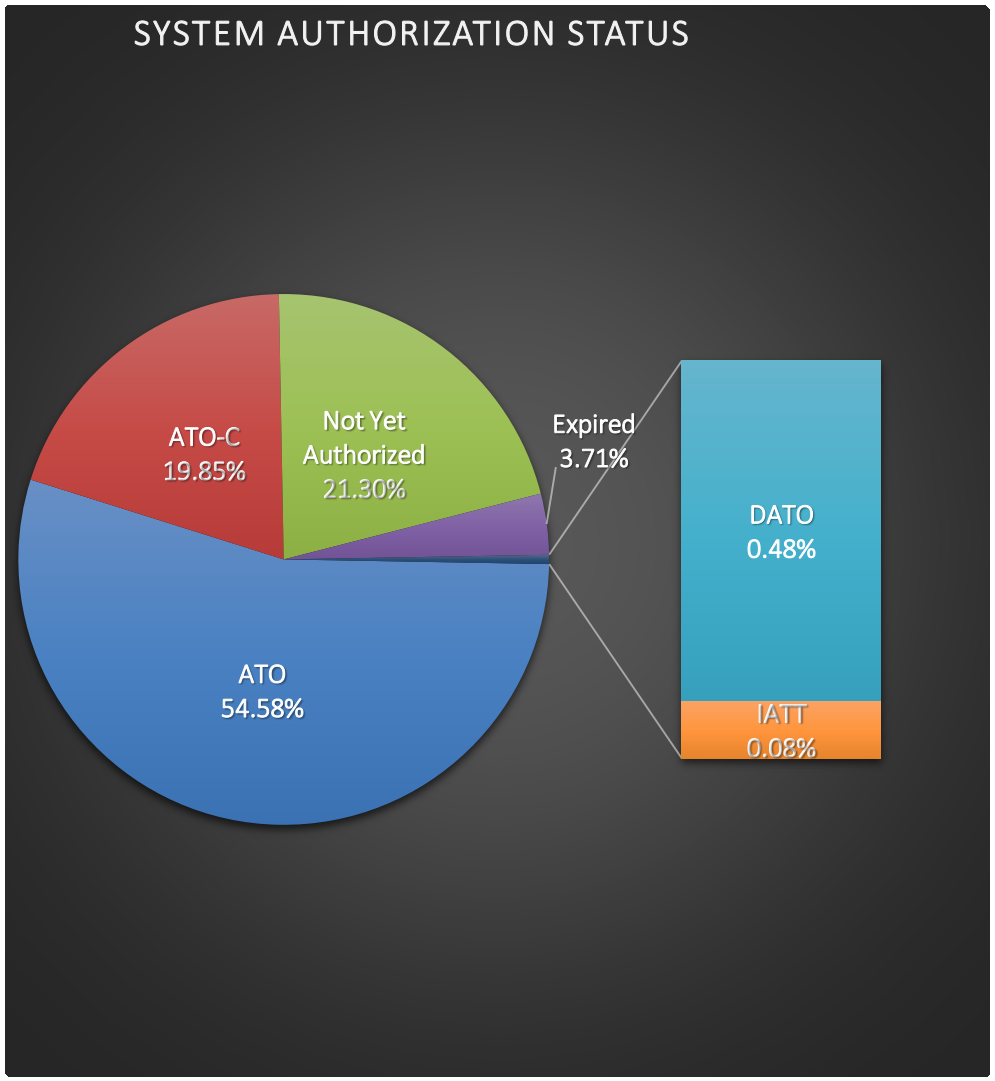
NAO Leadership

HQ CTP NAO

NAO: David Scott

Regional AOs

Eastern Region AO: Michele Fonville (Acting)
Central Region AO: William Vaughn
Western Region: Stacey Omo
Mid-Atlantic Region: Ezekiel Marshall



NISP eMASS Metric	
# Registered Systems in NISP eMASS	6,420
# of Authorizations Processed in FY21	3,473
# of NISP eMASS Users	4,079

Overview: The chart shows the percentage of all the systems within the NISP by authorization status. The following are the statuses: (1) Authorization To Operate (ATO), (2) ATO with Conditions, (3) Not Yet Authorized, (4) Expired, (5) Denial of Authorization to Operate (DATO), and (6) Interim Authorization to Test (IATT).

NAO COVID-19 Operational Adjustments

- Assessment and authorization activities continue to be performed by DCSA personnel.
  - ISSPs will perform security reviews of classified Information Systems per the DAAPM 2.2.
  - The only change is the execution of on-site security control assessment activity, which may be delayed, deferred, or rescheduled in consideration of local COVID-19 travel and visitation restrictions.
  - The resulting authorization decisions for operating classified information systems may result in an ATO, ATO with conditions (ATO-C) or an administrative extension of the ATD.
- Command Cyber Readiness Inspections (CCRI)
- Continued industry stakeholder engagements partnering to provide guidance, assistance as necessary to safeguard classified

Security Review Assessor (SCA) Triage

- RMF SCA Triage - initial plan review for completeness prior to complete ISSP risk assessment
  - Initial cursory review enables immediate corrections as necessary from industry
- Common errors: Artifacts, Risk Assessment and Test Results (common issue with test results, controls do not reflect they were retested to support A&A reauthorizations and controls do not explain the how)

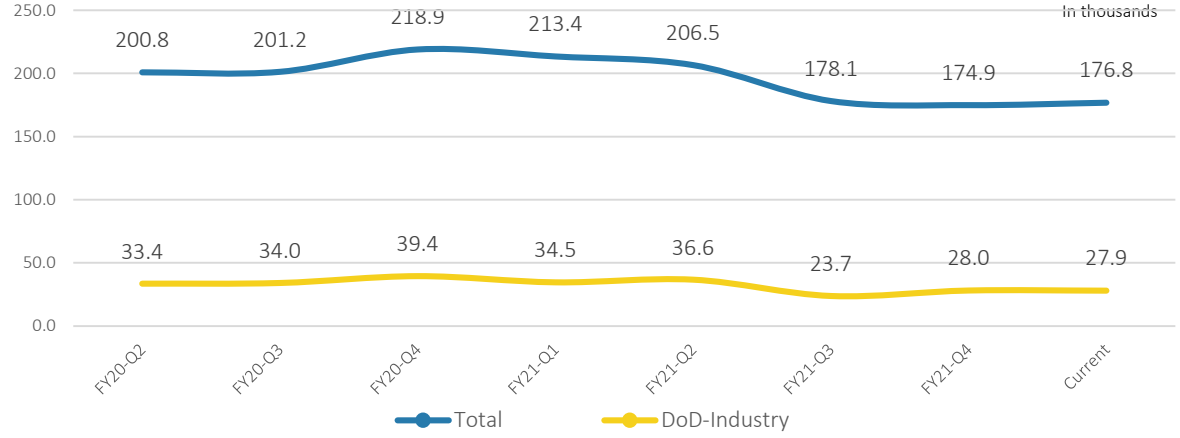
NAO – What is Next?

- Fiscal Year 2022 and Beyond
  - eMASS
    - Package Workflow enhancements (PAC)
    - Job Aids & additional guidance
  - DAAPM 3.0
    - Provide enhanced guidance & clarity for industry
    - Process improvements, identifying and addressing any gaps
  - NISP Connection Process Guide (CPG)
  - Command Cyber Readiness Inspections (CCRI)
  - eWANs – Enterprise WANs
  - Continued collaboration with NISP stakeholders

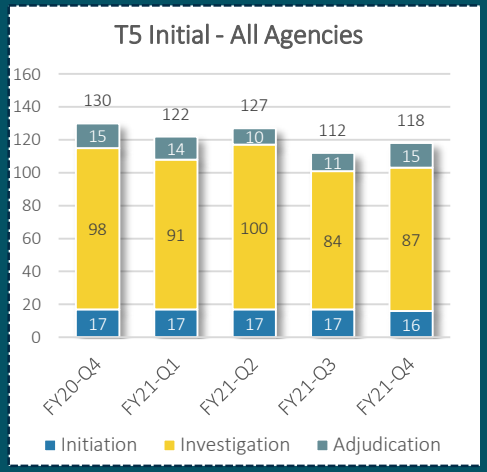
DCSA INVESTIGATION INVENTORY & TIMELINESS | *Industry*

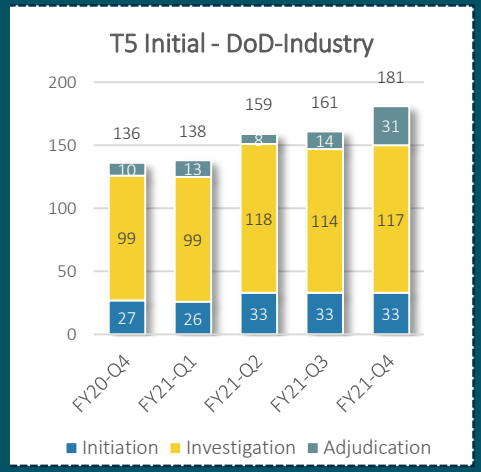
INVESTIGATION

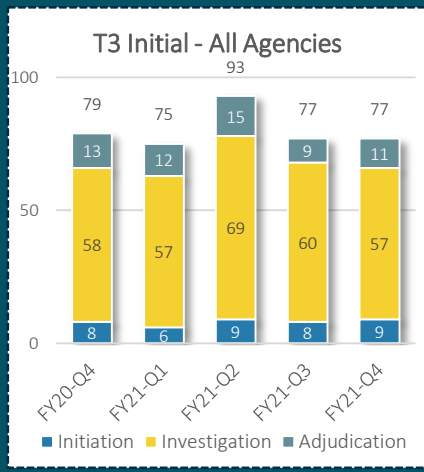
CURRENT INVENTORY	
All DCSA Customers	176.8K
Industry Only	27.9K

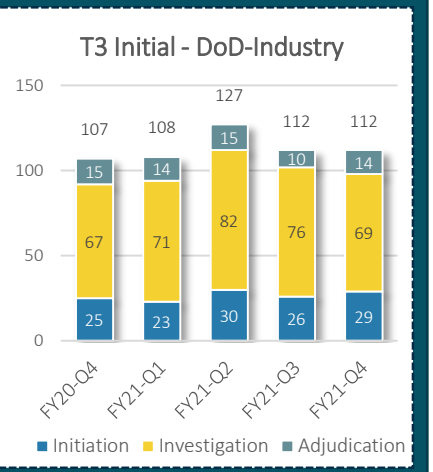


END-TO-END TIMELINESS (Fastest 90% of adjudicated investigations in days)









Data as of: 10/18/2021

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

FY21 PSI Execution

1M
NISP Contractors With Clearance Eligibility

Continuous Vetting

Over 975,000
Industry Subjects Enrolled in CV

~145,000
Industry PRs Deferred into CV to Date**

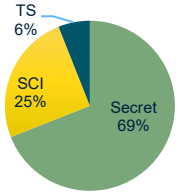
6%
Rate of CE Alerts Received

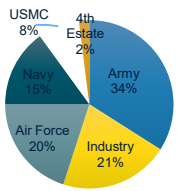
Early Detection

Early Detection and Risk Mitigation, before next PR due to begin

Secret: 7 Years 1 month

Top Secret: 2 Years 7 Months





CV ENROLLMENT GOAL

SUCCESS!!

Thanks for the Partnership

WHAT CAN INDUSTRY DO

Submit updated SF86 data if requested!

Follow guidance posted on DCSA website on Sep 2 2021

CV ALERT TRENDS

44K Valid Alerts
19K Actionable
43% not previously known
16K Unique Subjects

Majority Criminal and Financial

CV WAY AHEAD

TW 1.25 to TW 1.5

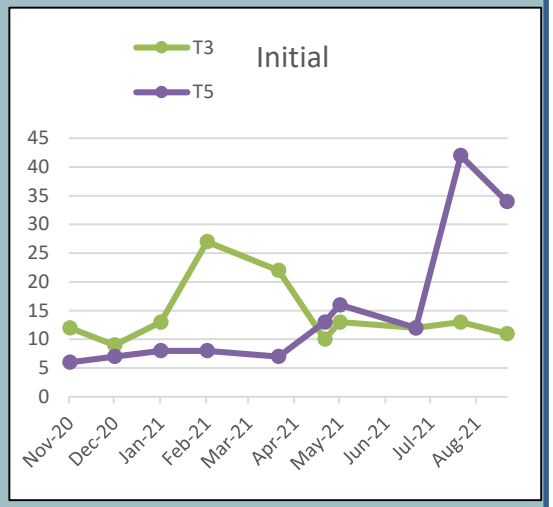
***Educate, Educate, Educate!**

ADVERSE INFO REPORTING

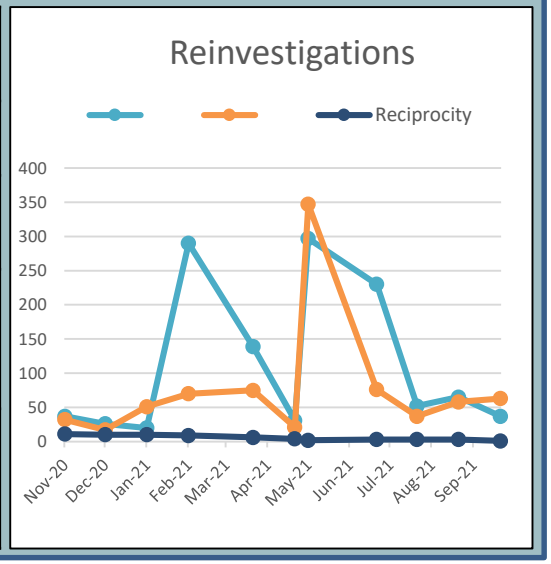
Adjudications (ADJ) For Industry

National Security Timeliness

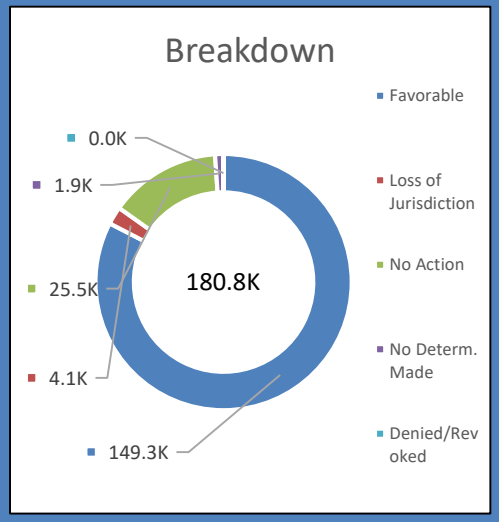
Historical Timeliness Initials	T3	T5
Current Month	13	22
One Year Ago	18	31
Two Years Ago	37	41

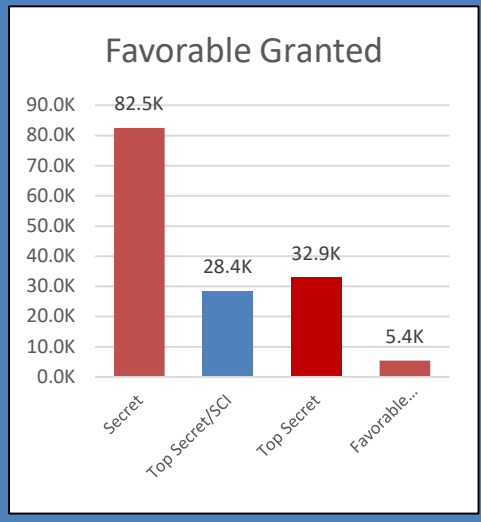


Historical Timeliness Reinvestigations	T3R	T5R	Recip.
urrent onth	27	63	1
One Year Ago	16	63	13
Two Years Ago	70	70	NA

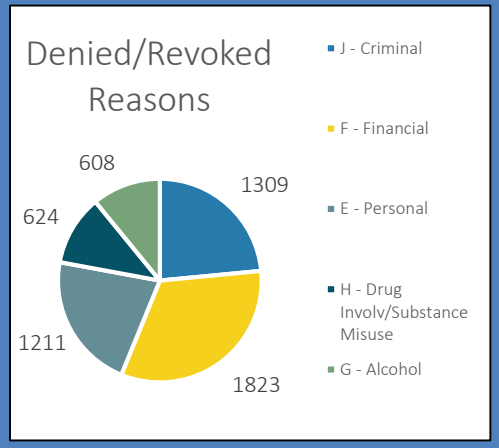


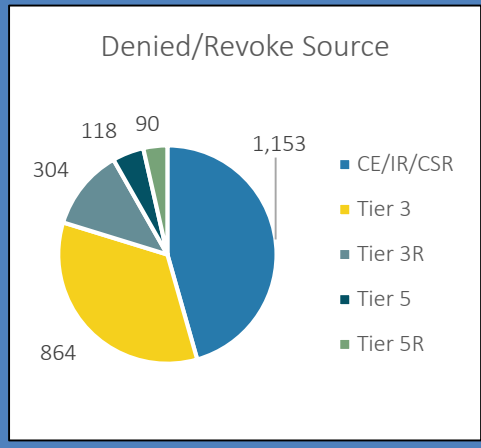
National Security Adjudications





Denied/Revoked

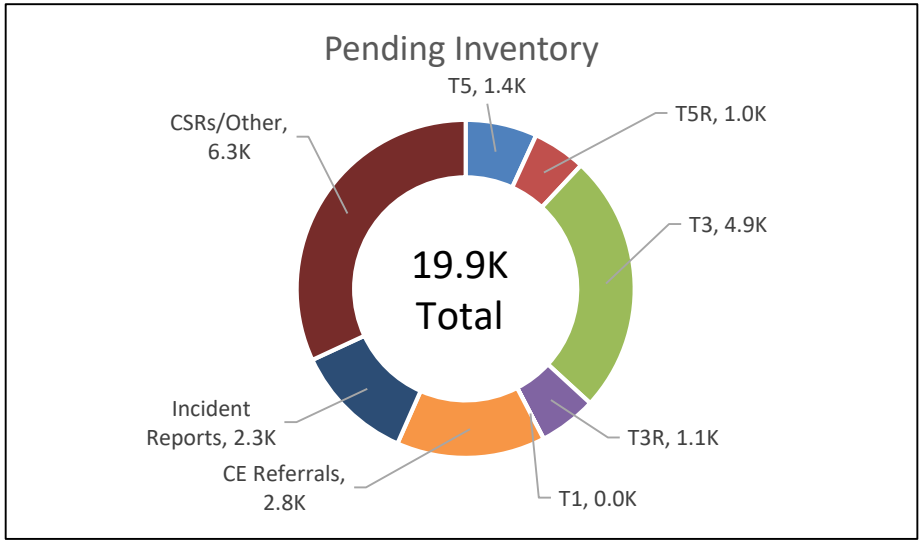


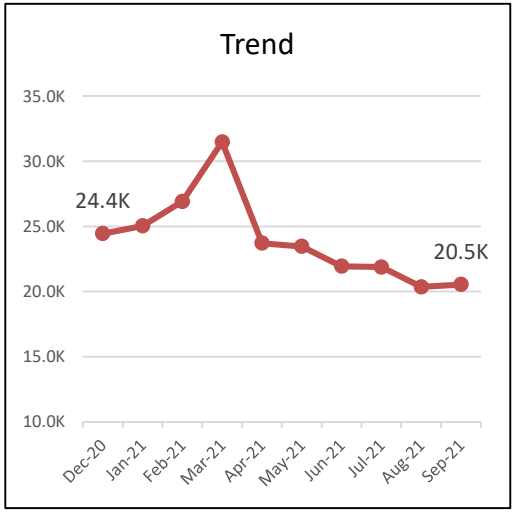


Report Date: 10/05/2021
OPR: DCSA ADJ Metrics Team

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Adjudications (ADJ) For Industry





Historical Inventory	
Current Month	19.9K
Last Month	20.4K
Last Year	38.4K

Monthly Closed	
Current Month	11.8K
Last Month	14.2K
Last Year	12.9K

Report Date: 10/05/2021
OPR: DCSA ADJ Metrics Team

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

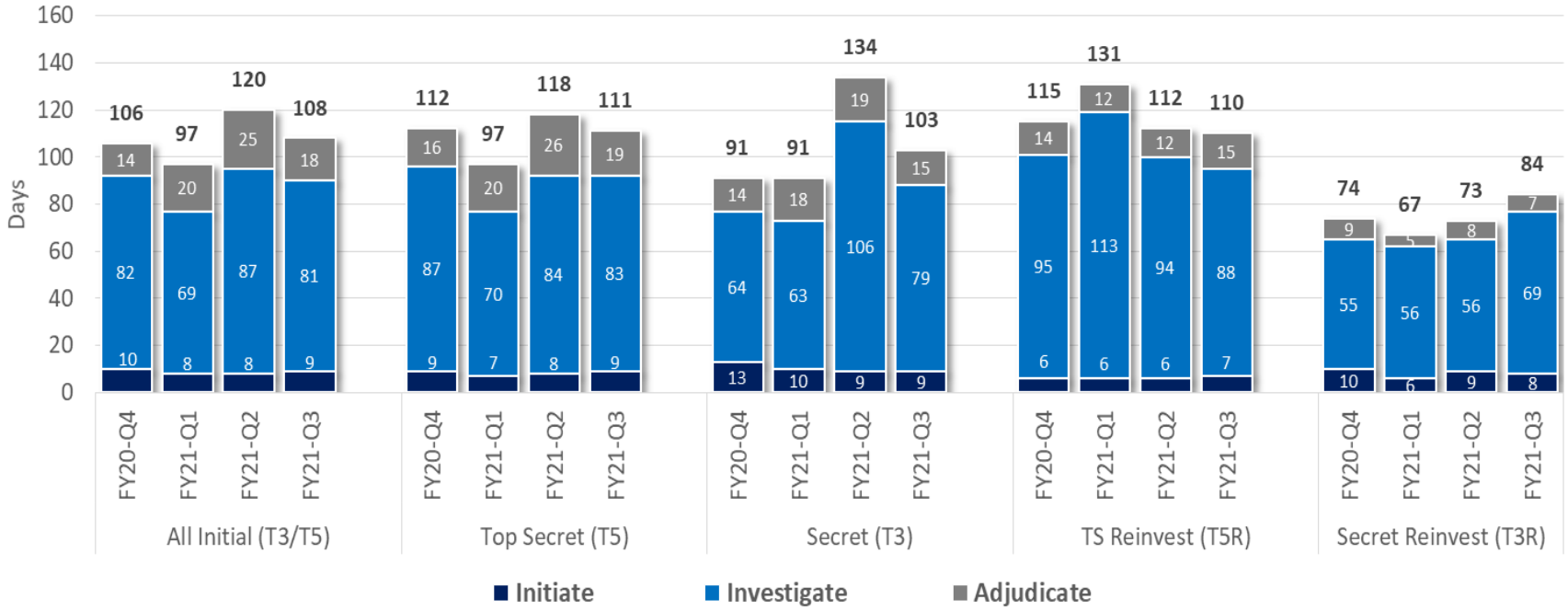
Workload & Timeliness Performance Metrics

Department of Energy

*Metrics provided by Defense Counterintelligence and Security Agency

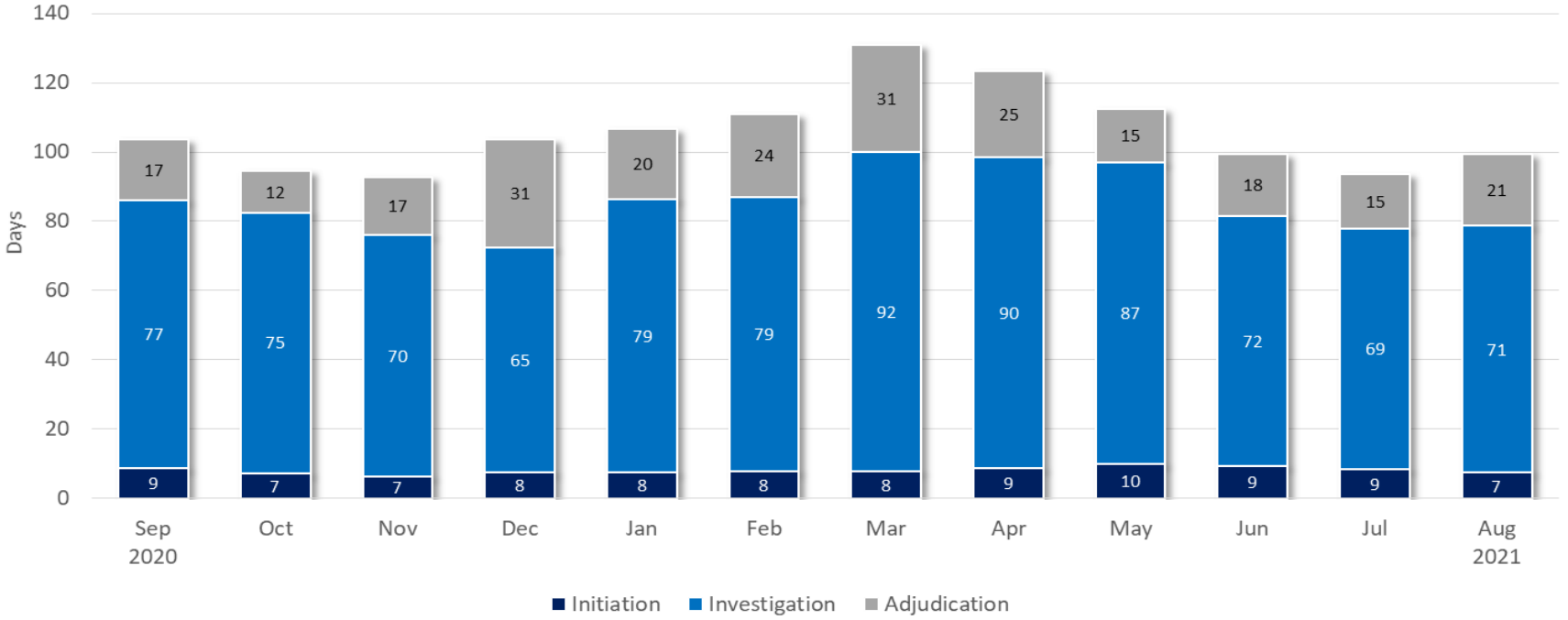
Quarterly DOE Timeliness Performance Metrics

Average Days for Fastest 90% of Reported Clearance Decisions Made



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations	Secret Reinvestigations
Adjudication actions reported – 4th Q FY20	1,716	1,346	370	1,883	576
Adjudication actions reported – 1st Q FY21	2,078	1,711	367	1,580	654
Adjudication actions reported – 2nd Q FY21	2,294	1,851	443	1,929	450
Adjudication actions reported – 3rd Q FY21	2,700	2,206	494	2,632	462

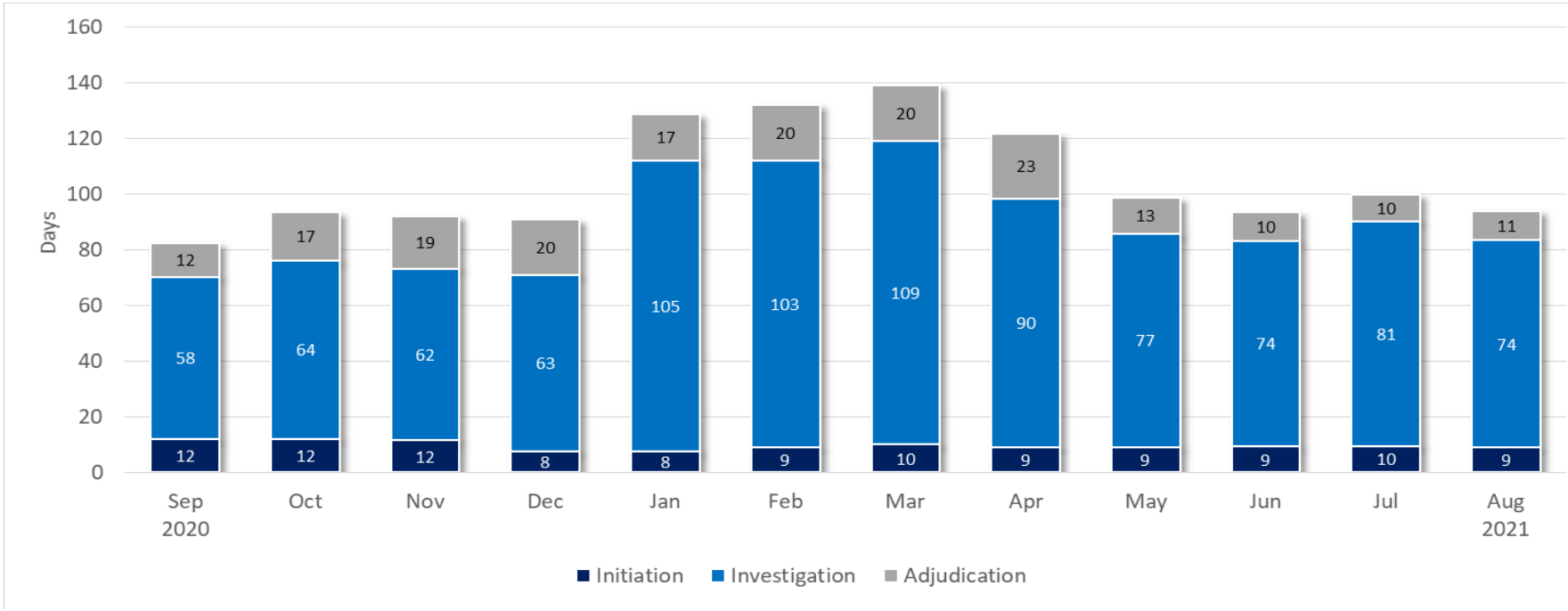
Monthly Timeliness for Fastest 90% of Initial Top Secret (T5) Security Clearance Decisions



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

	Sep 2020	Oct 2020	Nov 2020	Dec 2020	Jan 2021	Feb 2021	Mar 2021	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021
Total Adjudications Reported	453	577	478	656	557	550	746	776	625	805	749	718
End-to-End Timeliness (Fastest 90%)	104 days	94 days	93 days	104 days	107 days	111 days	132 days	123 days	112 days	99 days	93 days	99 days

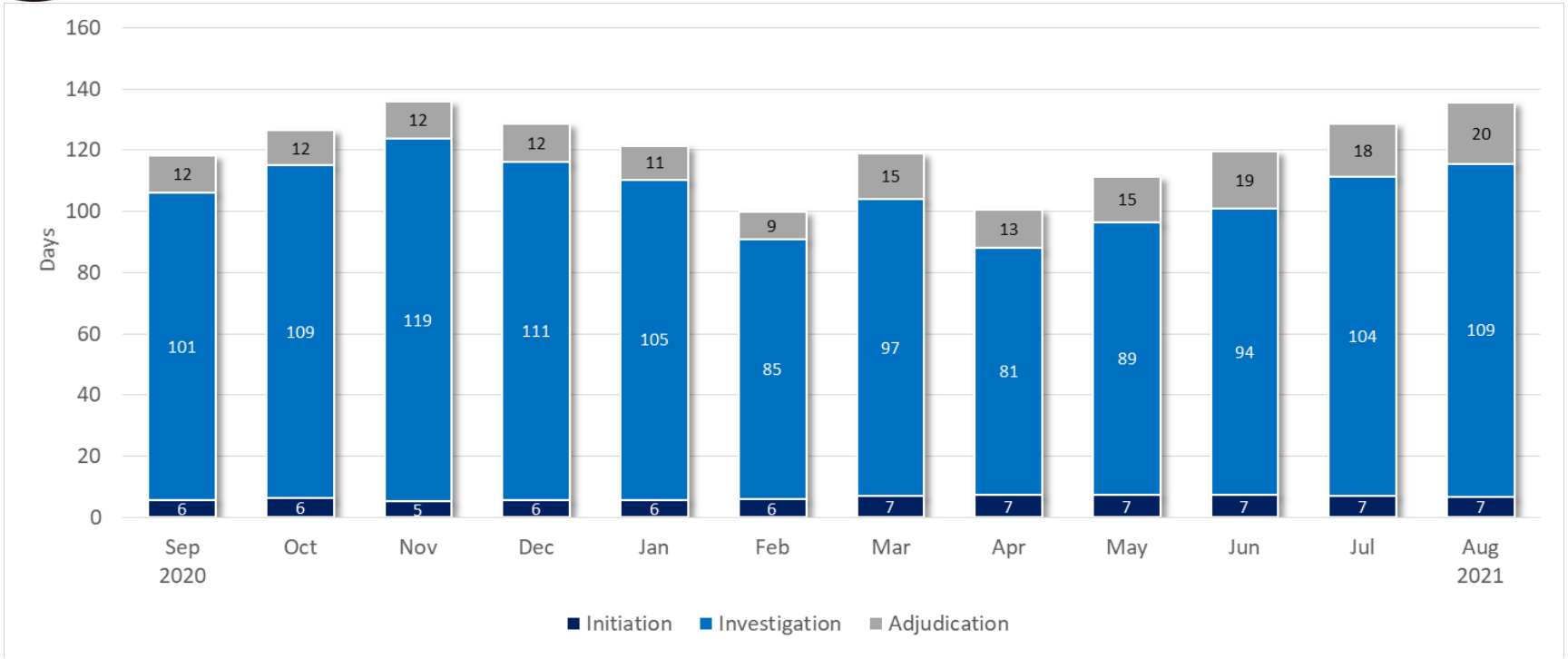
Monthly Timeliness for Fastest 90% of Initial Secret (T3) Security Clearance Decisions



GOAL: Initiation – 14 days *Investigation – 40 days* *Adjudication – 20 days*

	Sep 2020	Oct 2020	Nov 2020	Dec 2020	Jan 2021	Feb 2021	Mar 2021	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021
Total Adjudications Reported	146	151	114	102	134	126	183	152	148	194	211	212
End-to-End Timeliness (Fastest 90%)	83 days	93 days	91 days	89 days	127 days	132 days	139 days	122 days	99 days	93 days	101 days	94 days

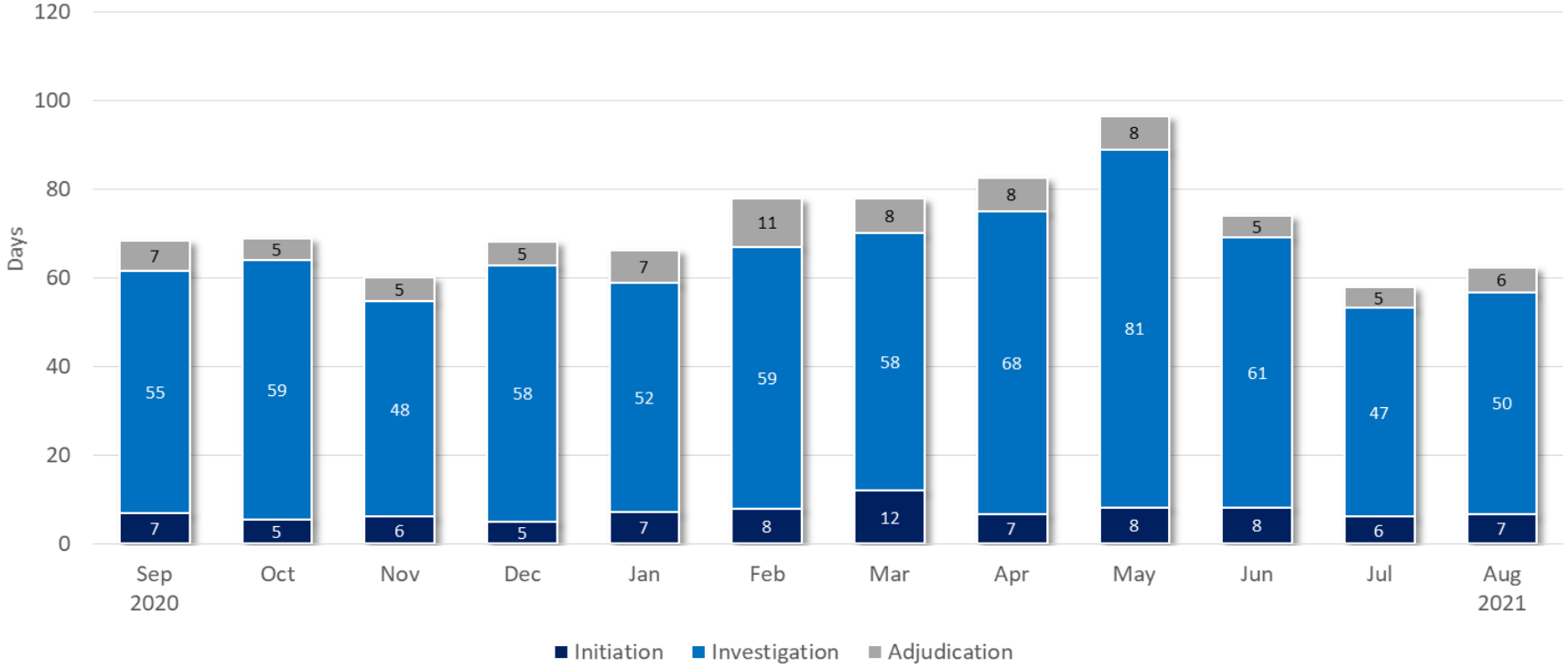
Monthly Timeliness for Fastest 90% of Top Secret Reinvestigation (T5R) Security Clearance Decisions



GOAL: Initiation – 14 days *Investigation – 150 days* *Adjudication – 30 days*

	Sep 2020	Oct 2020	Nov 2020	Dec 2020	Jan 2021	Feb 2021	Mar 2021	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021
Total Adjudications Reported	592	599	590	391	475	730	724	861	910	861	781	744
End-to-End Timeliness (Fastest 90%)	118 days	125 days	135 days	129 days	123 days	101 days	119 days	101 days	111 days	120 days	129 days	136 days

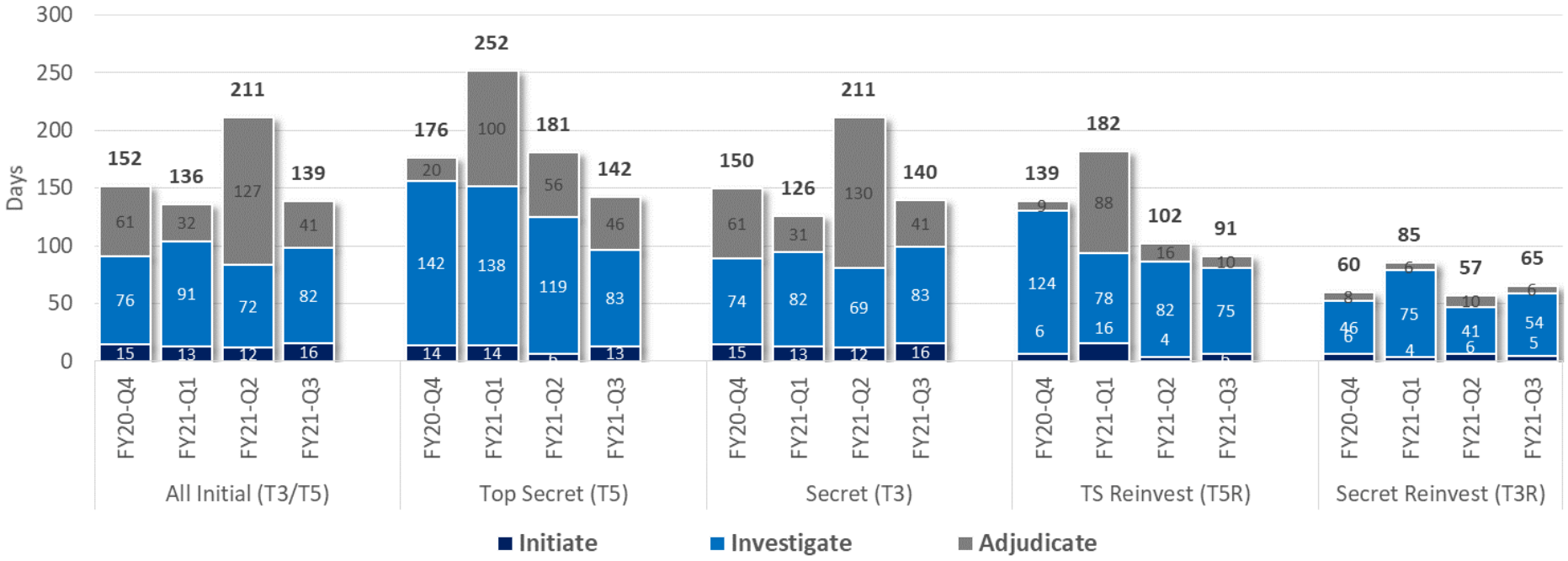
Monthly Timeliness for Fastest 90% of Secret Reinvestigation (T3R) Security Clearance Decisions



	Sep 2020	Oct 2020	Nov 2020	Dec 2020	Jan 2021	Feb 2021	Mar 2021	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021
Total Adjudications Reported	178	290	173	191	179	122	148	196	106	160	148	164
End-to-End Timeliness (Fastest 90%)	70 days	68 days	59 days	68 days	65 days	78 days	78 days	83 days	97 days	74 days	58 days	63 days

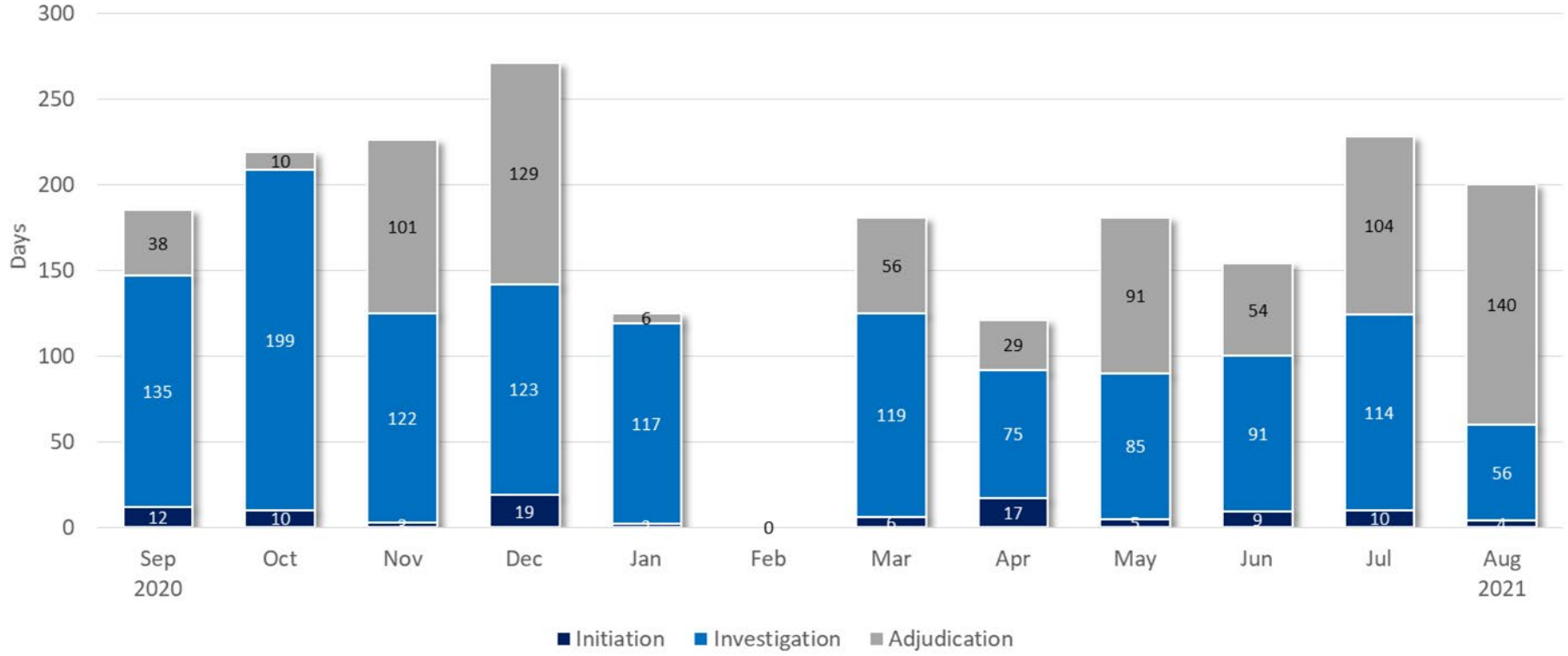
Workload & Timeliness Performance Metrics

Quarterly NRC Timeliness Performance Metrics



	All Initial	Top Secret	Secret/ Confidential	Top Secret Reinvestigations	Secret Reinvestigations
Adjudication actions reported– 4th Q FY20	55	5	50	5	25
Adjudication actions reported– 1st Q FY21	43	5	38	3	28
Adjudication actions reported– 2nd Q FY21	82	3	79	16	35
Adjudication actions reported– 3rd Q FY21	86	12	74	44	55

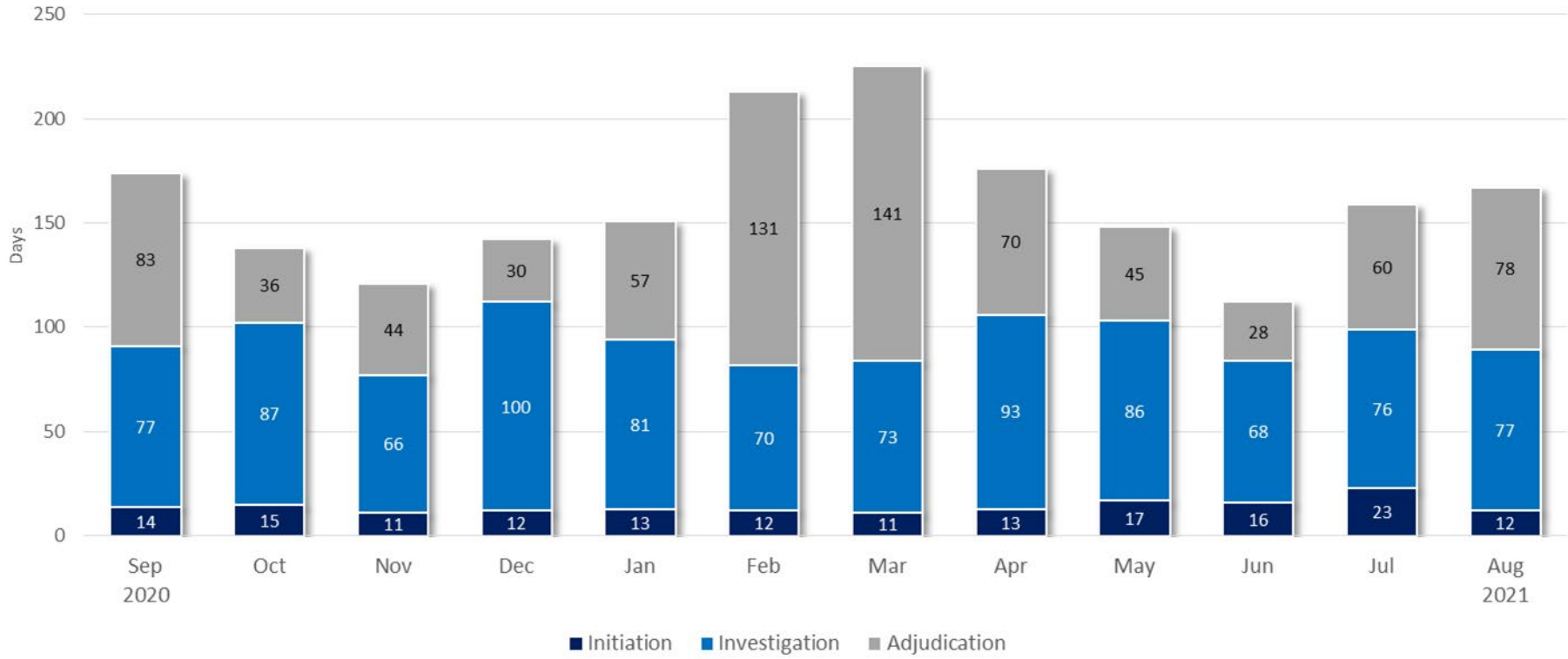
Monthly Timeliness for Fastest 90% of Initial Top Secret (T5) Security Clearance



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

	Sep 2020	Oct 2020	Nov 2020	Dec 2020	Jan 2021	Feb 2021	Mar 2021	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021
Total Adjudications Reported	2	1	1	3	1	0	3	5	1	6	4	3
End-to-End Timeliness (Fastest 90%)	185 days	219 days	226 days	271 days	125 days	n/a	181 days	121 days	181 days	154 days	228 days	200 days

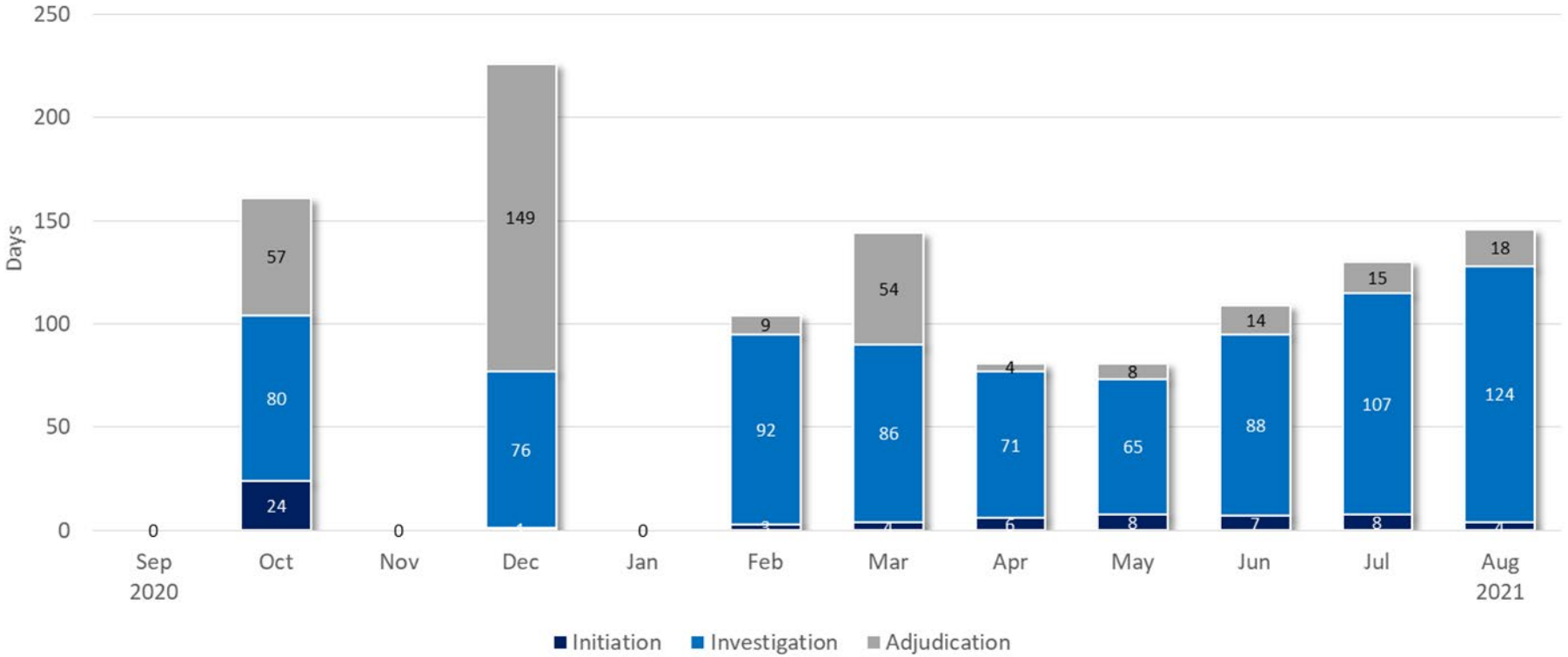
Monthly Timeliness for Fastest 90% of Initial Secret (T3) Security Clearance Decisions



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

	Sep 2020	Oct 2020	Nov 2020	Dec 2020	Jan 2021	Feb 2021	Mar 2021	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021
Total Adjudications Reported	20	13	10	15	17	18	48	22	24	27	38	31
End-to-End Timeliness (Fastest 90%)	174 days	138 days	121 days	142 days	151 days	213 days	225 days	176 days	149 days	112 days	159 days	167 days

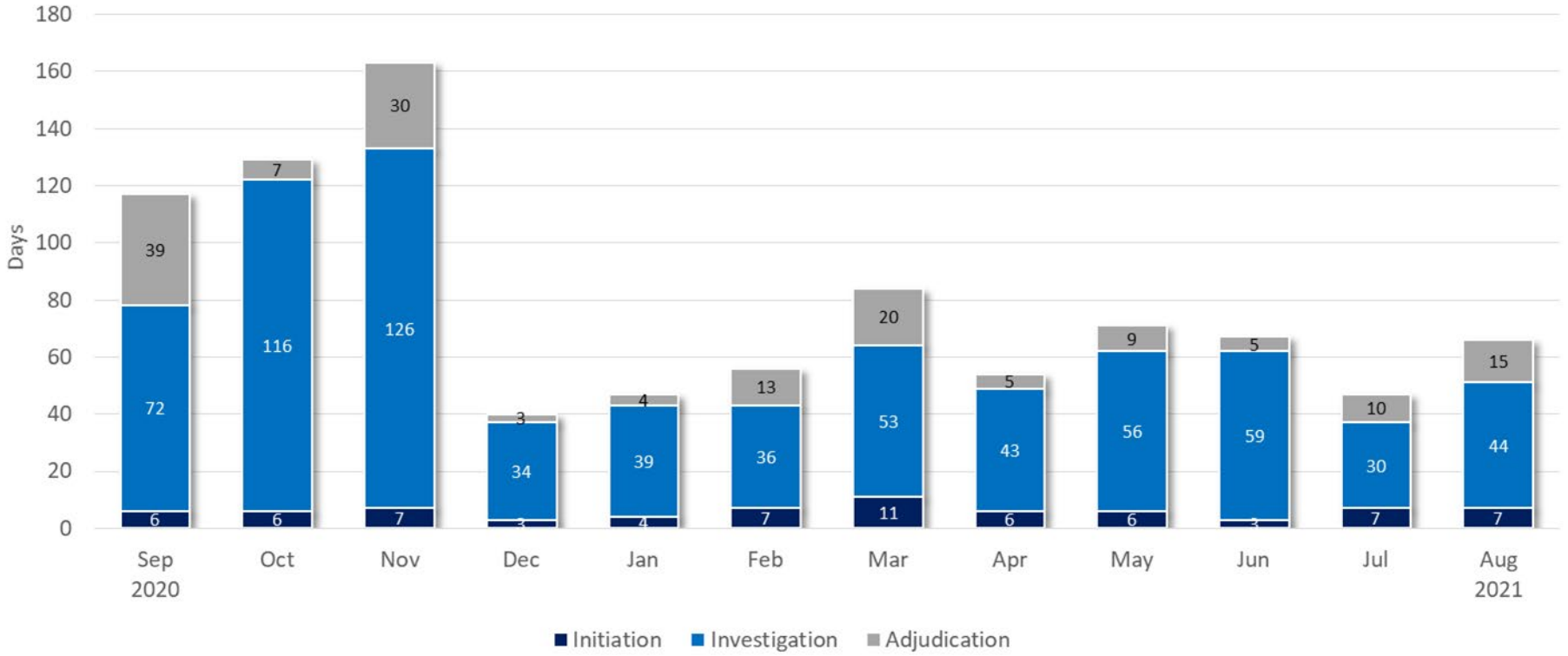
Monthly Timeliness for Fastest 90% of Top Secret Reinvestigation (T5R) Security Clearance Decisions



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

	Sep 2020	Oct 2020	Nov 2020	Dec 2020	Jan 2021	Feb 2021	Mar 2021	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021
Total Adjudications Reported	0	2	0	1	0	5	11	11	15	17	9	8
End-to-End Timeliness (Fastest 90%)	n/a	161 days	n/a	226 days	n/a	105 days	144 days	80 days	80 days	109 days	129 days	146 days

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



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

	Sep 2020	Oct 2020	Nov 2020	Dec 2020	Jan 2021	Feb 2021	Mar 2021	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021
Total Adjudications Reported	2	12	3	14	19	8	8	13	17	25	34	38
End-to-End Timeliness (Fastest 90%)	117 days	129 days	163 days	40 days	47 days	56 days	83 days	54 days	71 days	67 days	47 days	66 days

Information Security Oversight Office

Protect • Inform • Assess

NISPPAC Working Groups

- Clearance
  - NISPOM rule compliance in effect (8/24/2021)
  - TW 1.25 deadline
    - 9/30/2021 for full national security population entered
  - Last mtg 9/15/2021

- NISP Information Systems Authorization (NISA)
  - Discussed Solid State Device (SSD) Sanitization
  - Last mtg 3/31/2021

NISPPAC Working Groups

- FOCI (formerly called NID)
  - Discussed NDAA for FY 2019 Section 842, Removal of National Interest Determination (NID) Requirements for Certain Entities which stated a covered National Technology and Industrial Base (NTIB) entity operating under a special security agreement pursuant to the NISP shall not be required to obtain a NID as a condition for access to proscribed information beginning October 1, 2020
  - Last mtg 12/9/2020
- Cost
  - Gov't only at this time
  - Discussed how to collect costs of NISP for Industry
  - Last mtg 12/2/2020

NISPPAC Working Groups

- NISP Systems
  - Discussed the systems associated with the NISP program at the various CSAs
  - Last mtg 9/10/2020
- Insider Threat
  - Discussed training and certification of security professionals, insider threat plans, Section 9403 of the NDAA for FY 2021 (federal policy on the sharing of information pertaining to contractor employees in the trusted workforce)
  - Last mtg 9/2/2020
- Policy
  - Discussed 32 CFR 148 and 2004 Integration, reciprocity on NIDs
  - Last mtg 1/7/2020