National Industrial Security Program Policy Advisory Committee (NISPPAC) Meeting
Wednesday, April 14, 2021 - 10:00 a.m. - 1:00 p.m.
National Archives and Records Administration
Meeting held virtually

Agenda

Welcome, Introductions, and Administrative Matters	**10 mins**
Action Item Follow Up	**5 mins**
Reports and Updates	
Industry Update	**15 mins**
Department of Defense (DoD) Update	**15 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**
Break	**5 mins**
Cybersecurity Maturity Model Certification (CMMC) Presentation	**30 mins**
General Services Administration (GSA) Black Label Presentation	**30 mins**
Working Group Update	**10 mins**
Defense Office of Hearings and Appeals (DOHA) Update	**5 mins**
Controlled Unclassified Information (CUI) Update	**5 mins**
General Discussion, Remarks and Adjournment	**10 mins**

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.

Valerie B. Kerben

National Counterintelligence and Security Center
Office of the Director of National Intelligence

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

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

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

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

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

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

Tracy L. Kindle

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

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

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

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

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

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.

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.

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.

DANIEL MCGARVEY is the Senior Principle Business Process Analyst for Alion Science and Technology and is responsible for providing executive consulting in strategic planning for CI/Security programs supporting government and industry. He is the former Senior Consultant for Suitability and Security Clearance Performance Accountability Council, Program Management Office (SSCPAC/PMO). While there, in addition to developing the behavioral model for Personnel Vetting, he provided guidance to the PMO on how activities may be interpreted by stakeholder agencies and industry. Further, he is a senior instructor for the National Security Training Institute (NSTI), providing advanced training in Counterintelligence, Intelligence Collection, and Insider Threat.

He is an active member of the Intelligence and National Security Alliance (INSA) and the National Defense Industrial Association (NDIA), Industrial Security Division. As an American Society for Industrial Security (ASIS) International member, he was the Chair of the Chief Security Officer (CSO) Leadership Development Committee (LDC), Chair of the Defense & Intelligence Council and team lead for analytical development in the Insider Threat Working Group.

He is a retired member of the Defense Intelligence Senior Executive Service, as the Director, Information Protection, Office of the Administrative Assistant to the Secretary of the Air Force, Headquarters U.S. Air Force, Washington, D.C. He was responsible for the policy development, implementation, training and oversight of the Air Force's information, industrial and personnel security programs. He was chair of the Air Force Security Advisory Group and provided Secretariat support for the Air Force Security Policy Oversight Board. He was also the Functional Manager for the security career field and Chairman of the Air Force Security Advisory Council.

Prior to his Air Staff assignment, Mr. McGarvey was assigned to the National Reconnaissance Office (NRO) with duties that included the development of international space security policy; commercialization of space, a rotational assignment to the National Security Council as adjunct senior staff supporting both the Joint Security Commission II and the U.S. Security Policy Board; Chair of the Training and Professional Development Committee under the Policy Board; and Chief of the Training and Education Division.

As a career military intelligence officer, Mr. McGarvey was cross-trained and assigned in all functional areas. His assignments included a rotational tour as an infantry platoon leader followed by intelligence assignments at both the tactical and strategic levels.

Dennis Arriaga

Dennis is the Director of Security and Corporate FSO for SRI International, where he leads the diverse team responsible for developing, implementing, and administering security programs across the Institute. Dennis' security experience spans those involved in corporate security management, as well as those disciplines unique to industrial security within Department of Defense (DOD), Special Access Program (SAP), and Sensitive Compartment Information (SCI) arenas.

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 the Executive Director for Enterprise 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.

Mrs. Durkin was elected as a National Industrial Security Program Advisory Committee (NISPPAC) representative in 2020 and recently became 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 is also Vice Chair of the ISWG NRO Working Group.

Mrs. Durkin 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.

Deputy Assistant Director
NISP Authorization Office
SELENA P. HUTCHINSON
Defense Counterintelligence Security Agency

Selena P. Hutchinson, GSLC, has been the Deputy Assistant Director, NISP Authorization Office (NAO), Defense Counterintelligence Agency (DCSA) since April 2011. She has over forty years of information technology and cybersecurity management experience in diverse project management, systems acquisition, cyber security and leadership roles. She previously served as the DSS Chief Information Officer. DCSA oversees the protection of national security assets in the hands of industry and provides integrated security services to the Department of Defense. NAO is responsible for the implementation of risk management framework, Information Systems Security Professionals development and is usually the final authority on complex technical, assessment and authorization of systems, and cyber issues that require adjudication.

Ms. Hutchinson received her BS degree in computer information science from Alabama State University and received commission in the U.S Air Force where she had a variety of assignments including a teaching stint at Lowry AFB, CO; several years in the Pentagon engaged in various aspects of information technology, acquisition, and major program management. She ended her military career in 1990 after multiple Pentagon assignments including nuclear munitions support officer.

Ms. Hutchinson began her civil service career with the Federal Bureau of Investigations, where she was involved in the management of several forward leaning technologies in the law enforcement and intelligence communities. Ms. Hutchinson began her graduate studies at Auburn University, completed a Master's of Science Degree in Administration with Central Michigan University and later achieved the Global Information Security Certification. She is also a graduate of the Harvard Kennedy School's Cybersecurity Course. She served twice as Post Commander of the J.E. Hoover Memorial Post 56 of the American Legion and is still an active member. Ms. Hutchinson is an Executive Board Member of Community Lodgings, LLC, a local charity whose mission is to lift families from homelessness and instability to independences and self-reliance. She also participates in a number of other local volunteer programs.

BIOGRAPHY
DEFENSE INTELLIGENCE AGENCY
DEFENSE INTELLIGENCE SENIOR LEVEL

STACY S. BOSTJANICK

Senior Expert for Contracting

Ms. Bostjanick is currently serving as the OUSD A&S, Director of Cybersecurity Maturity Model Certification (CMMC) Policy. In this role, she is responsible for managing the initiation of the CMMC program and is responsible for establishing all Policy and Procedures with regard to the CMMC.

Previously, she served as the DIA, Head of Contracting Activity in which she was responsible for planning, managing, directing and accomplishing the total DIA procurement program. Ms. Bostjanick has also worked as a Senior Contracting Officer for the Missile Defense Agency on the Standard Missile 3 Block IA and IB development and production program. She was responsible for cradle-to-grave execution of over $5 billion of highly-complex, cutting-edge contracts for our nation's missile defense systems. Ms. Bostjanick has also served as the Deputy Procurement Executive with the Office of the Director of National Intelligence where she had responsibility for establishing Intelligence Community Enterprise-wide Policy and submissions to the Program Management Plan on an annual basis.

Ms. Bostjanick has had numerous awards and accomplishments throughout her career including the Naval Meritorious Civilian Service Award, David Packard Excellence in Acquisition Award, Office of the Secretary of Defense Certificate of Appreciation, the Director of National Intelligence Award for Collaboration Leadership, National Intelligence Meritorious Citation, and the Small Business Award.

Biography

U.S. General Services Administration

Christopher G. Pollock

Chief, Policy, Standards and Engineering Branch
Office of General Supplies and Services
Federal Acquisition Service
Supply Chain Management

Chris Pollock has been the Chief of the Policy, Standards and Engineering Branch of Supply Chain Management (SCM) for the General Supplies and Services (GSS) Portfolio of the Federal Acquisition Service since April 2018. In that position, he is responsible for managing the standards and engineering functions of GSA's procurement and distribution of consumable supplies to Federal agencies worldwide, with special emphasis on support for the U.S. military. Overall this program generates annual sales between $600M - $1.4B and up to 3 million business transactions a year.

Mr. Pollock also performs as the Program Manager for the GSA Security Equipment Program. This includes performing as the Chairman for the Interagency Committee on Security Equipment (IACSE) and serving as GSA's representative on the Security Equipment and Locking Systems (SEALS) Interagency committee. This committee develops Federal Specifications related to security equipment for the storage of classified information and weapons.

Mr. Pollock received a master's degree in Engineering Management from George Washington University in 1992 and a bachelor's degree in Electrical Engineering from The University of Maryland in 1989.

National Industrial Security Program Policy Advisory Committee (NISPPAC) Meeting Minutes April 14, 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 66th meeting on Wednesday, April 14, 2021 virtually. Mark Bradley, Director, information Security Oversight Office (ISOO), served as Chair.

Jeffrey Spinnanger, Director, Critical Technology Protection (CTP), Office of the Under Secretary of Defense for Intelligence & Security (OUSDI&S) discussed new National Industrial Security Program Operating Manual (NISPOM) rule. Public comments continue to be adjudicated around 60% of which came from Industry partners. The key issue they are going through with the comments are related to Security Executive Agent Directive (SEAD) 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position. Some of the amendments are expected to deal with Trusted Workforce (TW), National Interest Determinations (NIDs)/Section 842 of NDAA 2019.

The SEAD 3 Industrial Security Letter (ISL) went out for NISPPAC comments, of which were extensive. ISLs now go through the Office of Management and Budget (OMB) before being released.

There's been a lot of discussion on Federal Information Systems as it is described and defined in Volume 2 of DoD 5200.22. In the past, Federal Information Systems were previously referred to as "guest systems", which meant a system approved by another government organization. DCSA has authorized federal systems in the hands of cleared industry for many years, however, some government customers are reading the volume two federal information systems paragraph as the only way to adhere to policy for their systems, which DoD thinks is not the case. If Industry or government customers are told to disconnect a previously approved system, please raise the issue with the regional authorizing officials who will engage this directly.

When it comes to Solid State Devices (SSDs), the Defense Counterintelligence and Security Agency (DCSA) follows DoD 5200.22, Volume 2 guidance, which allows flexibility for the government information owner to accept sanitization risk, rather than destruction. If industry has specific sanitization products or questions to address or utilize, submit them directly to NSA for evaluation or the government customer for further guidance.

Section 847 of the Fiscal Year (FY) 2020 National Defense Authorization Act (NDAA) included a requirement for assessment of beneficial ownership pertaining to foreign ownership, control, and influence (FOCI) for DoD prime and subcontracts that are more than $5 million in value. It requires a DFARS clause that will go through the rule-making process, however, in advance of that process, DoD is drafting a DoD instruction. It is presently in the internal coordination phases within the DOD components under OUSDI&S.

DoD is sponsoring a project with the Applied Research Laboratory for Intelligence and Security (ARLIS) to explore the use of commercial classified cloud in the NISP. ARLIS is going to conduct a pilot, working

with a small number of NISP companies to independently evaluate the connections and approvals process. The project builds on observable improvements to inter-operability, cybersecurity, and core requirements for information security in insider threat, user activity monitoring for highly classified IC and DoD requirements pertaining to compartmented programs that are already in work today, and exploring how those can meet similar application and requirements are presently executed under the NISP.

Heather Sims, Industry Spokesperson, briefed on behalf of Industry. NISPPAC Industry elections are coming up in September. If interested in one of the two open positions, contact a current industry member, or a Memorandum of Understanding (MOU) member.

32 CFR Part 117 is currently a major focus of industry while they move to implement and also adjust to the new changes. It is recommended to go through the new NISPOM for what is there and what is not there.

Another priority for Industry has been working with Performance Accountability Council Program Management Office (PAC PMO), Office of the Director of National Intelligence (ODNI), and Office of Personnel Management (OPM) as TW 2.0 continues to mature.

A third priority for Industry is the continued information sharing struggle. Industry is challenged with sharing of adverse information of cleared employees, potential insider threats identified by the government, target threats against companies, and Industry products and services provided to the government. Industry would like to have continued engagements with their government partners to talk about how information sharing can be increased. Industry is also challenged with being able to share known threats between companies without fear of reprisal and lawsuits. Information sharing with industry holistically is a challenge and improvements would strengthen their ability to provide better security mitigation strategies.

Industry is preparing for the implementation of a new NISPOM, managing and validating and correcting data in DISS, anticipating such a workforce 2.0, preparing for CMMC assessments, and trying to manage the role of controlled unclassified information (CUI).

While CUI is not a part of the NISP, there will be an impact by CUI implementation oversight. Industry is already experiencing a bifurcation of the programs. Each federal agency has been charged with developing a CUI program, but then Industry is dealing with each agency's varied interpretation. Each program is coming up with their own set of rules, leaving Industry in the middle of managing expectations. Industry needs better oversight of government agencies to ensure consistent approaches levied on Industry.

Keith Minard, Senior Policy Advisor, Critical Technology Protection, Defense Counterintelligence and Security Agency, provided the DCSA update.

ISLs are there to help clarify, interpret and provide guidance for industry to better implement portions of the NISPOM requirements. DCSA developed and fielded a NISPOM rule cross-reference tool that enabled readers to select known sections of the current NISPOM and it takes the user to the portion of the rule that it aligns. The tool can be found on the CDSE website. DCSA has been putting out webinars about the NISPOM changes and SEAD 3 reporting requirements.

DCSA has added an external facing webpage, https://www.dcsa.mil/mc/ctp/NISPOM-Rule/. It is intended to be a single source to the NISPOM rule information, key changes, events, links to tools and policy, and frequently asked questions for postings related to NISPOM rule to better enable its implementation. They are also using social media to put out updates about the rule. They also released a video called Get Ready for the Rule. It gets to some of the key changes in the NISPOM rule.

DCSA completed a scrub of their existing ISLs and identified some that have to be reissued sometime in the near term. Not all existing ISLs will remain.

DCSA is working to ensure their field personnel are have a consistent message on the rule. DCSA field personnel will not begin overseeing the new NISPOM rule until its implementation date.

With the onset of COVID-19 travel restrictions, DCSA shifted from mega operations to remote only activities. Their first priority was the health and safety of our workforce and yours. Secondarily, they focused on maintaining support to facilities and continued to conduct oversight responsibilities. COVID limited their ability to physically conduct onsite actions. For example, ATOs were issued without the necessary onsite review. Virtual closed area approvals and administration inquiries were conducted virtually. The first priority, when DCSA can safely begin scheduling onsite contractor visits, will be actions that have been delayed over the past year. This would include final assessments and approvals of storage that have been done without onsite validation, review of information systems that need verifications, and review of corrective actions.

Valerie Kerben, Senior Security Advisor, Special Security Directorate (SSD), National Counterintelligence and Security Center (NCSC), ODNI, provided the ODNI update.

The new Director of National Intelligence, Ms. Avril Haines stated during her confirmation that security clearance reform will be a high priority.

January 15, 2021, OPM and ODNI, as the Executive Agents (EAs), signed a joint Executive Correspondence (EC) on TW. This EC shifted from the prior phase of TW, where the EAs worked to reduce the investigation inventory. The shift to phase two of TW 2.0 focuses on policy development for the implementation of the new government wide approach, with different levels of policy covering the personnel vetting process from beginning to end. One of the main topics in the EC was providing guidance for the executive branch departments and agencies on the differences between TW 1.25 and TW 1.5 transitional state and the enrollment milestones. The EAs are working to ensure agencies are capable and ready to enroll in one of these transitional states. The ultimate goal for transitioning now is that continuous vetting will satisfy the traditional periodic reinvestigation (PR) process. So there will no longer be traditional PRs every five, 10 years. All employees in the national security population and those contractors will be enrolled in a continuous vetting capability where ongoing checks will be done. By September 30, 2021, all departments and agencies must enroll their full national security population in at least the TW 1.25 capability. By September 30, 2022, all departments and agencies must enroll their full national security population in the TW 1.5 capability. There are a few different capabilities regarding which record checks are being done and certain things the agencies are also responsible for doing. EAs are helping agencies enroll and ensuring their concerns are addressed during the implementation phase.

NCSC released a statement regarding COVID-19 and how mental health impacts should not impact national security eligibility. Counseling and undergoing treatment as a result of COVID or the associated

stresses should not in itself be considered a negative or disqualifying factor for rendering eligibility or access to classified information.

OPM issued clarifying guidance on marijuana use and reiterated the federal drug-free workplace that the adherence to the federal laws of using marijuana is illegal.

ODNI continues to operate with limited staff due to COVID-19. Even though they are not back to business as usual, they still have a lot of staff working on team type of schedules. They are operational and ready and able to respond to questions and concerns. Response times may be a little longer. The Scatter Castles program and Continuous Evaluation System help desk personnel are still available and they are fully operational.

Regarding the NISPOM rule implementation, DNI and CIA are working together to implement the NISPOM rule and retract any references to the prior NISPOM manual.

Rob McRae, Director of the National Security Services Division and Rich DeJausserand, Deputy Director for Industrial Security to the Department of Homeland Security (DHS), provided the DHS update. Their workforce largely posture largely remains in a telework remote work environment with the exception of law enforcement, border operations, and port operations.

DHS receives a majority of their industrial security services from DCSA, however, they continue to work with DCSA on the implementation of the new NISPOM final rule, specifically, working with the personnel security team in regards to SEAD 3. They are developing and implementing communication plans, developing policy documents, developing reporting tools, or in the process of developing reporting tools for SEAD 3. They continue to work with DCSA for FOCI assessments regarding accepting NIDs. While they will still conduct their own risk assessments with NIDs, they will make a risk management decision, based on our risk assessments we are still in the process of developing and working hand in hand with DCSA.

Mr. Mark Hojnacke, Director of Security Policy at the Department of Energy (DOE), provided the DOE update. DOE has compared the NISP CFR requirements against DOE's current security requirements and has noted a number of areas that will be addressed, either by page changes to the security directives or through secretarial policy memoranda, including the NIDs language from the recent NDAA update. The DOE Acquisition Regulation (DEAR), and its security clause references DOE security directives, rather than the NISP, to account for other security assets within the department. Because it does not specifically address the NISP, there is no need to update the security clause, although there will be other updates to the DEAR to address NIDs and FCL processing.

DOE's current operating status is that they continue maximum telework throughout DOE in compliance with the OMB goal to operate at 25% of normal building occupancy.

Chris Heilig and Denis Brady provided the NRC update. Their volume of cases and adjudication timeliness is stable. NRC was able to continue processing cases because their process is primarily electronic. As COVID restrictions are easing, we're able to take care of drug tests and fingerprinting at almost a normal pace again. NRC continues to regulate the civilian use of commercial nuclear energy in academic and medical use. The NRC is continuing to implement the requirements of the NISPOM, but had to come up with alternative means for conducting that, but working with our industry stakeholder partners, they have been able to achieve those goals.

Most of NRC is in phase two for maximum telework, but some of their regional offices still are in our phase one for mandatory telework, but are still able to conduct our functions as the regulator for nuclear energy.

Stacy Bostjanick, Director of Cybersecurity Maturity Model Certification (CMMC), briefed updates to the CMMC policy. They are continuing to work through the rule making process, and are adjudicating the comments. Based on those comments, they have gone back and looked at the model and are considering some possible changes in response to those questions and comments, but they are not ready to publicize what those are.

They are moving forward with their pilot and getting the Certified Third-Party Assessor Organizations (C3PAOs) assessed at the CMMC level three, as they consider the information that they are pulling together with those assessments as being sensitive information. Every assessment that they accumulate and review will be housed in the DISA GovCloud, and that information will then be ported over to the Supplier Performance Risk System (SPRS) where contracting officers and program managers will have the opportunity to go in to validate that companies have the appropriate CMMC level for the contracts that they're competing on. They have had a couple of pilots that have canceled. Some of them had award dates in June and the C3PAOs were not going to be ready in time. One of the main tenets of their pilot is they are not going to impact the timing of any of the award cycles for acquisitions right now. They have set up a supply chain working group with members of OUSD, across OUSD and the services, to come up with a lexicon and taxonomy and a standardization to look at supply chain risk and how to assess it and mitigate it and then what are the tolerance levels that can be expected.

Roy Jusino, with the DoD Lock Program, and Chris Pollock with GSA, briefed about recent policy that addresses the removal of older GSA approved containers and vault doors that are currently used for protection of classified information. At the end of service, the removal date is between 2024 and 2028.

Mark Bradley and Greg Pannoni, Associate Director, ISOO, briefed about the NISPPAC working groups (WGs). There was discussion about the Small Business Administration (SBA) joint business venture final rule. ISOO is still working through concerns with it. There will be a forthcoming ISOO notice that clarifies entity eligibility requirements for joint venture entities that enter into classified contacts with the federal government. TW's ongoing transition to 2.0 was discussed, the JPAS to DISS transition, the NISPOM changing over to a rule and the implications of some of the changes, particularly SEAD 3, but also a little bit on TS accountability, limited FCLs, and the intrusion detection recognition that not just UL 2050, but other entities that meet Nationally Recognized Testing Laboratory (NRTL) standards. There was a little bit of discussion about security vulnerability assessments, the ratings, how that's evolving ratings for SBAs. For the NISP Cost WG, this is a broader sub element to an initiative that ISOO under has undertaken, beginning about two or so years ago, to refine and simplify, to support agencies in their efforts to provide overall data with respect to their classified national security information programs, as required by executive order and directive to ISOO on an annual basis. One that get the most attention was reporting on the estimated numbers of derivative and original classification activities, which in and of itself was a highly suspect number. ISOO suspended the collection of data while working on refining collection efforts, consolidating them and taking advantage of technology. ISOO is talking about cost incurred by contractors under Cognizant Security Agency (CSA) cognizance. The government has met several times. Before ISOO brings Industry in to see what has been come up with, ISOO wants to hear from each CSA to bring their proposal for how they intend to gather costs that their NISP contractors incur. Each CSA can come up with something that they all agree on and just have one mechanism. We

do not want to have duplication of cost collection. Keeping with the overall intent of the reform effort for data collection, ISOO wants to keep it as simple as possible, so once we have the CSAs' way ahead, and some degree of consensus, we would then bring NISPPAC Industry into take a look at what we have and to get their input.

During the NISP Information Systems Authorization (NISA) WG, we discussed SSDs.

David Scott, DCSA, briefed DCSA NISA WG information, which was provided with slides.

Marianna Martineau, DCSA, briefed DCSA investigation and adjudication information, which was provided with slides. For the background investigation group, as COVID continues, they are maximizing telework as most staff are already working remotely, and we are continuing to use the executive agent approved alternative processes, including telephone interviews. At the beginning of COVID-19, DCSA evaluated their processes and implemented a hold where they were not receiving responses to their requests for additional information or other actions related to COVID-19. They re-evaluated current operating procedures and are reinstating pre-COVID business processes and procedures regarding correspondence requirements for responses. They will no longer be issuing indefinite automatic extensions related to the COVID-19 pandemic. Subjects, through their security managers and facility security officers, will have 30 days from the date request, for an action in the Defense Information System for Security (DISS) to comply with that official request for information. If you have any questions, please send them to DCSA through the portal.

Tracy Kindle, DOE, provided the DOE personnel security update. They are meeting the Intelligence Reform and Terrorism Prevention Act (IRTPA) timeliness goal for all investigative tiers.

Chris Heilig, NRC, provided the NRC personnel security update. They are meeting the IRTPA timeliness goal for all investigative tiers.

Perry Russell-Hunter, Director, Defense Office of Hearings & Appeals (DOHA), provided DOHA's update. 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. Calendar year 2020 was the highest average year for total numbers of Statements of Reasons (SORs) reviewed and issued since 2016. SORs are still going out in typical numbers and are timely. They currently have 330 SOR reviews pending, which is a typical number. At the end of January, they had 390 pending. DOHA reviewed and the CAF issued over 3,100 draft SORs during the period between March of 2020 and March of 2021. The first four months of FY 2021, they reviewed and DoDCAF issued 1,200 SORs. There is going to be a shift later this year where DOHA will begin providing and tracking the SORs directly to Industry employees.

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 where were DOHA needed to reach, DOHA has now tested and is making 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.

Evan Coren, Implementation Lead for CUI, ISOO, briefed on ongoing CUI efforts. The National Information Exchange Model (NIEM) has released NIEM 5.0, which for the first time includes a CUI

metadata standard. NIEM is one of the common metadata standards. This will significantly improve the metadata consistency that occurs as metadata is used in association with CUI. The CUI Registry Committee and ISOO will serve as the mechanism to update and review changes to the CUI domain within. National Institute of Standards of Technology (NIST) Special Publication (SP) 800-172 has been published. This was formerly known as the draft NIST SP 800-171B. NIST 800-172 recommended security protections for non-federal information systems that process or transmit CUI. It was finalized February 2, 2021. It mainly evolves changes in narrative and boundaries and does not change the controls that are in place. The controls within NIST 800-172 are used in the CMMC Level 4 and Level 5 determining that contractors have the necessary controls in place.

The CUI Federal Acquisition Regulation (FAR) clause is projected to go out to public comment later this year. Once it is out for comment, ISOO will hold an ad hoc stakeholders meeting that will be scheduled at the beginning of the public comment period to address concerns and discuss the draft version that will be up for comment.

Everyone is encouraged to take a 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 next NISPPAC is scheduled for October 27, 2021. 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

- DCSA is still in process of internal and formal coordination of an Industrial Security Letter (ISL) on Insider Threat Program, which will replace ISL 2016-02. STATUS: CLOSED due to all ISLs being reviewed due to the NISPOM rule.

- Schedule insider threat working group meeting. STATUS: CLOSED. The meeting was held on September 2, 2020.

- DCSA needs to find out if they will be responsible for all SCIF accreditations or just those associated with DIA. STATUS: CLOSED. DSCA, will have a responsibility for the accreditation of military departments, 4th Estate, and their contractor SCIFs.

Questions and Answers from the NISPPAC

None

NISPPAC Attendance

Abbott, Aprille
Abeyta, Melissa
Abney, Quantoinette
Abrams, Nikki
Ackerman, Daniel
Adam, Macvean
Adams, Elizabeth
Adams, S. Ann
Adissu, Mekdes
Agnew, Daniel
Akers, Lynetta
Albalos, Raven
Alcala, Anna
Alexander, Christine
Alexander, Treva
Allen, Nicole
Ambrose, Zorica
Andablo, Yvette
Anderson, James
Andrews, John
Anthony, Christopher
Aquinas, Jennifer
Arffman, Kathryn
Argumedo, Lori
Armstrong, Robert
Arriaga, Dennis
Arvidson, Alex
Ashby, Holli
Ashley, Janet
Atkinson, Stephan
Auldridge, Kelly
Avila, Donna
Babic, Adriana
Backhus, Annie
Bailey, Robert
Baldree-Nichols, Amelia
Barbee, Lisa
Barr, Julianna
Barry, Tris
Bassey, Dunamis Gospel
Bauer, Sandra
Baugher, Kimberly
Baxter, Jordan
Bean, Joan
Belcher, Lara
Belsinger, Deborah
Bensie, Evelyn
Benson, Michael
Bentel, Misty
Bentley, Nathaniel
Bergeman, Stephen
Berry, Kathleen
Beske, Jamon
Bethea, Nasu
Bhalla, Ginny
Biggers, David
Black, Christina
Blacka, Leslie
Blackmon, Robin
Blais, Steven
Blake, Theresa
Blakslee, Jen
Bland, Booker
Blanton, Yvette
Blauch, Dana
Blazic, Andrew
Blazich, Brigid
Bledsoe, David
Blount, Richard
Boaston, Thomas
Boccalino, Michael
Bock, Kristy
Bodrick, Detra
Booker, Patrick
Boomer, Mindy
Borrero, Rosie
Bosket, Jeffrey
Bostjanick, Stacy
Boston, Bridgette
Boulware, Chelsi
Boyd, Michelle
Bradley, Mark
Brady, Denis
Brandt, Elizabeth
Braxton, Kishla
BrennanFontes, Jean
Britton, Charles
Broadie, Constance
Broglin-Bartlett, Darinda
Brokenik, Trish
Brooks, Valerie
Brooks, Beverly
Broussard, Derrick
Brown, Alexis
BrownWard, Joy
Bruce, Erin
Bruder, Bethany
Bryan, Karen
Bryant, Penny
Budnik, Caroline
Bunch, David
Burger, David
Burgos, Sasha
Burke, Doris
Burns, Lynn
Burrell, Lisa
Burton, Stacie
Busch, Melissa
Byrge, David
Cabe, John
Call, Samantha
Callier, Jewel
Calloway, Victor
Campbell, Parry
Cannady, Richard
Cantie, Lacey
Capsalis, Corey
Cardella, Thomas
Carlin, Michelle
Carnaghi, Suanne
Carney, Jacqueline
Carter, Roxanne
Casey, Sandy
Cashin, Joseph
Cassidy, Kerry
Castel, Jason
Cavanagh, Nicole
Cavano, Jeffrey
Chambers, Steven
Chamblee, Tamra
Chapman, James
Chappell, Curtis
Charyton, Dianne
Chaumont, Luis
Chituras, Jimmie
Choate, Kevin
Christian, Laurie
Christian, Heather
Church, Brenda
Chvotkin, Alan

Cinelli, Giovanna
Clader, Heather
Clark, Wade
Clasen, Melissa
Claus, Matthew
Clifford, Debra
Cline, Nathan
Clohessy, Meaghan
Cloud, Brian
Cobble, Jonall
Coburn, Catherine
Cole, Jim
Cole, R. Keith
Coleman, Jeff
Coleman, Johnathan
Collo, Robin
Colon, Susan
Condon, Jessica
Connelly, Michael
Connerley, Christopher
Conquest, Karlyon
Conway, Scott
Cook, Krista
Cooper, Nicole
Cooper, Teresa
Coren, Evan
Coulter, Sarah
Couts, Dustin
Crawford, Priscilla
Crew, Kimberly
Crickenberger, Joy
Crouch, Alan
Cullison, Ashley
Curcic, Odeyra
Da Cruz, Emilea
Dahle, Nissa
Dangel, Alex
Daniels, Trudy
DAnthony, Stacey
Dartsch, Kelly
Davis, James
Davis, Glynn
Dawson, Michelle
Dawson, Steven
Dean, Mary
Deck, Rob
Dejausserand, Richard
Dejesus, Matthew
Delgado, David
Demers, Michael
DeMong, Jeremy
Denegal, Robert
Deramus, William
DiazMartinez, Sarah
Dickman, Jessica
Diggs, Brenda
Dinkel, Jane
Disante, Pete
Dixon, Beth
Donnelly, Janet
Dotson, Virgil
Drew, Paul
Duke, Christina
Dukoff, David
Durant, Kelly
Durkin, Tracy
Dyer, Teresa
Eckel, Mark
Eckerstrom, Suzanne
Eddins, Kristina
Edge, Kimberly
Edington, Mary
Edmonds, Tracy
Edson, Mark
Ellison, Lori
Enabnit, Misty
Engelbrecht, Laura
England, Michael
Epps, Danette
Equels, James
Erickson, Heather
Escobar, Sheri
Escobar, Michael
Escobedo, Robert
Estes, Megan
Everett, Trina D.
Ewton, Erin
Fabozzi, Madeline
Falk, Suzanne
Faller, Mike
Farmer, Anne
Farmer, Andrea
Fehlner, Scott
Feldman, Ben
Fell, Rob
Fergus, Jeffrey
Fisher, Darci
Fisher, Ray
FitzEnz, Jonathan
Flaherty, Joann Emma
Flaminio, Stephanie
Fleischmann, Derek
Flewellen, Linda
Flores, Stephanie
Flores, Mayra
Ford, Elizabeth
Fowler, Don
Fowler, Pat
FrayCarlson, Kerry
Fredrich, Cathy
Freeman, Lisa
Fritts, Kaitlyn
Fulco, Joseph
Funicello, Kasey
Funicello, Lorena
Fuster, Kathleen
Gabeler, Jennifer
Gainey, Mitch
Gannaway, Mary
Garcia, Vincent
Gardner, Kelly
Garner, Bryan
Garner, Byron
Garner, Carol
Geisler, Angela
George, LaVerne
George, Kelly
Gibbs, Diane
Gibbs, Katrina
Gibson, Sharon
Gilbert, Daniel
Ginder, Linda
Glassic, Scott
Gleason, Kimberly
Goldstein, Donald
Gonzalez, Benjamin
Good, Suzanne
Goodwin, George
Graham, Jennifer
Gray, Juaquita
Gray, Tonya
Greaver, Angela
Green, Heather
Green, Neil

Greene, Gus
Greenebaum, Rebekah
Gribble, Gene
Griffe, Gene
Griffin, Diane
Grimes, Daniel
Grinsell, Caitlin
Gulack, Jeffrey
Gunn, Lesley
Hadwin, Lisa
Haggerty, Paul
Hagood, Kenneth
Haire, Tamara
Haley, Rene
Hamilton, Jill
Hamilton, Pamela
Hargis, Jeremy
Harne, Joseph
Harris, Tamara
Harris Pagan, Heather
Harrison, Kimberly
Hartburg, Craig
Hayward, William
Heaton, Pamela
Heil, Valerie
Heilig, Chris
Helton, Alicia
Henderson, Alexis
Henderson, Kaila
Herbert, James
Herbst, Jonathan
Hernandez, Josh
Hertzog, Conrad
Hewlett, Daisha
Hill, Brett
Hill, Jessika
Hinojosa, Carla
Hodges, Hope
Hogan, Susanne
Hohauser, Michelle
Hojnacke, Mark
Holland, Betsey
Hollandsworth, Matt
Hollingsworth, Danielle
Holloman, Noelle
Holmberg, Brandon
Howar, Laura
Howard, Mark
Howell, Mark
Huber, Donna
Hughes, Kimberly
Hughes, Rachel
Hulet, Michael
Hunt, Matthew
Hurtt, Samuel
Husker, Frank
Hutcheson, Amy
Hutchinson, Selena
Hutchison, Alicia
Hyater, Sharon
Illidge, Kaitlin
Indelicato, Charles
Isely, Constance
Izadi, Katayoun
Jackson, Sonja
Jackson, Stephen
Jackson-Marquard, Kirsten
James, Robert
Jenkins, LeeAnn
Jensen, Kathryn
Jett, Christina
Jiggetts, Lauren
Joe, David
Johnson, Derrick
Johnson, Craig
Jones, Derek
Jones, Kenneth
Jones, Melinda
Jones, Cecilia
Jongema, Linwood
Jusino, Roy
Kamilova, Kamilya
Kaohi, Catherine
Karkoski, Michael
Kay, Jasmine
Kennedy, Beverlee
Kerben, Valerie
Kerr, Julie
Khajehali, Collette
Kidd, Linda
Kim, YuJin
Kimmel, Kim
Kindle, Tracy
King, Christyne
Kirby, Jen
Kitchens, Barbara
Kitts, Karen
Klaczyk, Joseph
Klink, Carolina
Knarr, Matthew
Koslow-Verdi, Alison
Kostielney, Craig
Kozacek, Shelly
Kraus Jr, Joseph
Kuethen, Bonnie
Kuo, Chia-Chi
Kyzer, Lindy
Lai, Kuan
Lamont, Kimberly
Lamps, Jeremy
Lancaster, Laura
Lanzillo, Brittany
Laperle, Deanna
Lapre, JeanPierre
LaRocque, Laurie
Lavallee, Stacy
Lawhorn, Jeffrey
Lawley, Sean
Lawrence, Mitch
Lawson, Pamela
Laybourne, Krista
Leadbeater, Holly
Lederle, Alan
Lee, Jessica
Lee, Amy
Leggiere, Eric
Lerma, Patricia
Lettera, Brenda
Levy, Isabelle
Lewis, Natasha
Lewis, Tiffany
LHeureux, Ann Marie
Lightner, Carol
Limon, Katherine
Lincoln, Kathryn
Lindsey, Andrea
Liner, Marquiz
Litscher, Theresa
Lomeli, Michelle
Lopa, Mary-Jane
Lord, Ginger
Lorenz, Lori
Lotwin, Andrew
Lowy, David

Lucock, Cynthia
Ludwick, Mark
Luera, Xanne
Luladakes, Carol
Lumber, Deborah
Lundquist, Margaret
Lupo, Tracy
Ly, Dan
Mace, Bernadette
Mackey, Shelton
Makthepharaks, Ironsy
Malbone, Nicole
Malloy, Barbara
Manglona, James
Mardaga, Heather
Marks, Laura
Marks, Michael
Marocco, Sandra
Martens, Sheri
Martin, Price
Martin, Kenneth
Martin, Susan
Martineau, Marianna
Martineau, Robin
Martinez, Hazel
Martone, Laura
Massaro, James
Mate, Edith
Matthews, Will
Mayercin, Elizabeth
Maylone, Angelica
Mazanec, Jeffrey
McCloud, Adrienne
McCoy, Linda
McDuff, Tiffany
McGarvey, Dan
Mcgregor, Arlene
McKay, Jennifer
McKenna, Danielle
McLaughlin, Stephen
Mclaughlin, Angela
McLeod, Donna
McLeod, Risa
Mcmanus, Daniel
Mcmillian, Toni
Mcnamara, Carrie
Mcnichol, Lindsey
McRae, Robert
Mctighe-Wetstein, Breanne
Measures, Lisa
Mechem, Stormie
Medina-Creel, Tina
Mencin, Brett
Metcalf, Jessica
Metz, Erin
Meuret, Kathy
Mignogna, Christal
Miller, David
Miller, Dean
Miller, Kevin
Miller, Susie
Miller, Mark
Minard, Keith
Mitchell, Adam
Mitchell, Bruce
Mitchell, Mary
Mitchell, Stephen
Mittleman, Elaine
Molnar, Kimberly
Mongold, Jamie
Morales, Alana
Morris, Christine
Morrissette, Virginia
Moseley, Paula
Moses, Zephaniah
Mosher, Leandra
Moshos, Phyllis
Moss, Leonard
Mucha, Lynn
Mullenax, Meredith
Mullenniex, Kelley
Muskett, Phillip
Nane, Amy
Needle, Kandace
Nelson, Wanda
Nelson, Ronald
Nguyen, Camtu
Nguyen, Chris
Nguyen-Huu, Valentine
Nickel, Robin
Nigro, Benjamin
Norman, Diane
Norris, Felicia
Nunley, Anne
Nunn, SeKitha
Nylander, Elsa
Obernier, Jennifer
Ogrysko, Nicole
Olson, Ashley
Opilla, Hunter
Oppenhagen, Christine
Orr, Mary
Oshita, Scott
Ososkie, Charles
Ou, Patti
Page, Tamara
Palmar, Jose
Palme, Jacob
Pannoni, Greg
Pappas, Joyce
Parker, Andrew
Parker, Rebecca
Parr, Doris
Parr, Justin
Partridge, Diane
Pashoian, Norman
Patterson, Jennifer
Pekrul, Mark
Pelen, Erick
Pelletier, Joe
Peritore, Chad
Perkins, Paul
Perrault, Judy
Persinger, Jonathan
Peyton, Kristy
Phagura, Satminder
Phalen, Charles
Phan, Xera
Pherson, Kathy
Phillips, Earl
Phillips, Wynn
Piccioni, Geraldine
Pickering, Tamiko
Pineda, Audrey
Pinson, Jenny
Pollock, Chris
Porter, Lizet
Posey, Mozelle
Potts, William
Pound, Mary
Powers, Kyla
Prell, Joseph
Price, Colleen K.
Prichard, Tennille

Pritchard, Gregory
Provencher, Marguerite
Pulliam,Donna
Pyles, Larry
Quintana, Sandra
R, Nora
Radloff, Steve
Ragland, Nicole
Raju, Clara
Ramaswamy, Shobha
Ramer, Cindy
Ramirez Perez, Yamirka
Randall, Sheila
Randor, Jason
Rarig, Karl
Reardon, Amy
Reck, Sydney
Reff, Royal
Regan, Margaret
Reidy, Lisa
Rendon, Annabelle
Renzella, Allyson
Reynolds, Catherine
Rheault, Chandra
Rhine, Carl
Ricci, Cheryl
Rich, George
Richardson, Urline
Riches, Daniel
Rickell, Cathy
Riggins, Rebecca
Rivera, Zulma
Rixmann, Tracy
Roche, Matthew
Rodgers, Mike
Rodriguez, Chamagne
Rodriguez, Adrian
Rogers, Geraldine
Rosera, Stephen
Roska, Camille
Ross, Stephanie
Rossiter, Lisa
Rousseau, Kelly
Rowen, Michael
Roy, Robyn
Runkle, Gretchen
Russ, Bill
RussellHunter, Perry
Sadler, Gregory
Samuels, Al
Sanchez, Elizabeth
Sanchez, Sunni
Sanders, Chikita
Santiago, Eduardo
Saylor, Julie
Scaramozzino, Shelley
Scattone, Russell
Schneider, Scott
Schneider, William
Schools, Patricia
Schuler, Shellie
Schultz, Joe
Scott, Christopher
Scott, David
Scott, Yvette
Scott, Beth
Scovel, Yen
Sease, James
Settles, Christina
Shade, Karl
Shanahan, Bonnie
Shedlock, Heather
Sheffield, Eleanor Harriet
Shelby, Kayla
Shimamura, Judy
Silveira, Cynthia
Sims, Heather
Sims, Taniesha
Singh, Kulvinder
Singletary, Patrice
Singleton, Naim
Sixkiller, Carolyn
Sjodahl, Debbie
Slicker Bobby, Lori
Slinko, Luke
Sloan, William
Smasal, Eileen
Smith, Anthony
Smith, Crystal
Smith, Jessica
Smith, Kelly
Smith, Susanne
Smith, Paula
Smith, Berette
Smith, Scott
Smith, Crystal
Smoot, Teresa
Solomon, Priscilla
Soltis, Sheldon
Soriano, Rojohn
Speace, Garrett
Spencer, Chuck
Spilman, Pamela
Spinnanger, Jeffrey
Stall, Camilla
Stanley, Terence
Starkey, Regan
Steele, Jessica
Stehlik, Terry
Steinbuch, Michael
Steinke, Sue
Steinour, Jason
Stell, Michael
Stellflug, Michelle
Stephens, Tracy
Stephens, Brooke
Stephens, Tod
Stewart, Michael
Stine, Olivia
Stolkey, Chris
Stone, Cheryl
Stovall, Fletcher
Stubbs, Marguerite
Stull, Sarah
Sugrue, Laura
Sullivan, Elisha
Sullivan, Karen
Sumpter, Valerie
Sura, John
Suter, Kenneth
Sutphin, Michelle
Swann, Gayle
Sydnor, James
Sylver, Ferroza
Sylvester, Steven
Taft, Dianne
Tarantino Setneska, Valerie
Tate, Charles
Tavakoli, Mahshid
Taylor, Lisa Dawn
Teemley, Kate
Tench, Charles
Terrell, Shatonna
Theriault, Jason

Thibault, Crystal
Thibodeaux, Kristie
Thoma, Jeff
Thomas, MaryJo
Thomas, Monika
Thomas, Donna
Thomas, Antoinette
Thomas, Katherine
Thomas, Grant
Thompson, Donna
Thompson, Blinda
Thompson, Michelle
Thornton, Diana
Thornton, Samantha
Tiffee, Brad
Tillson, Aric
Timmons, Katie
Tran, Kat
Trehern, Deborah
Tringali, Robert
Tsukamoto, Krystina
Tweed, Michael
Ty, Emmanuel
Ulery, James
Unruh, Carolyn
Uperesa, Dane
Vaccariello, Jeffrey
Vachon, Jackie
Van Horn, Valora
Vance, Robert
Vaughan, Tom
Vaughan, Francesca
Vaughn, Susie
Victoria, Elizabeth
Villa, Christopher
Villemaire, Doreen
Villescas Hermosillo, Jessica
Vilven, Shanna
Volak, Martha
Wackenhut, Molly
Waddle, Jill
Wagner, Bekah
Wahl, Tamara
Wallace, Charlene
Wallerson, Diane
Ward, Amanda
Ware, Laura
Warner, Jean
Warren, Kerry
Washington, Keshia
Watkins, LaTasha
Watters, Michelle
Weatherby, Bradley
Weaver, Gail
WeaverLillard, JoAnda
Webber, Joann
Weeks, Jeannine
Wells, Matt
Wendell, Jeremy
Wendt, Suzy
Westley, Allen
Wever, Xiomara
Weyrauch, Richard
Whelan, Mary
White, Carole
White, Iryna
White, Dorie-Ann
Whitteker, Mark
Wilkes, Chelsey
Willbanks, Ann
Williams, Enita
Williams, Jennifer
Williams, Maurice
Williams, Kristin
Wilson, Denise
Wilson, John
Wilson, Michelle
Wilson, Jennifer
Winch, Celestine
Winford, Donneaka
Winn, Terrance
Winton, Tracy
Wisnosky, Roger
Witherow, Leneda Kay
Wojciechowski, Kathy
WojcikBerthelotte, Brooke
Woldridge, Marya
Wood, Delvin
Wood, Lemy
Woodall, Christopher
Woodard, Teresa
Woodfolk, Torri
Woodruff, Patricia
Woolsey, Wailohia
Worsham, Robert
Wright, Amy
Wright, Paula
Wuest, Heather
Wunderich, Daren
Wyatt, Stacy
Yenigun, Katie
Yeow, Kim
Yersak, John Patrick
Young, Erin
Zeigler, Bobby
Zeitler, Erin
Ziemienski, Jason
Zubrick, Sarah
Zweil, Alison

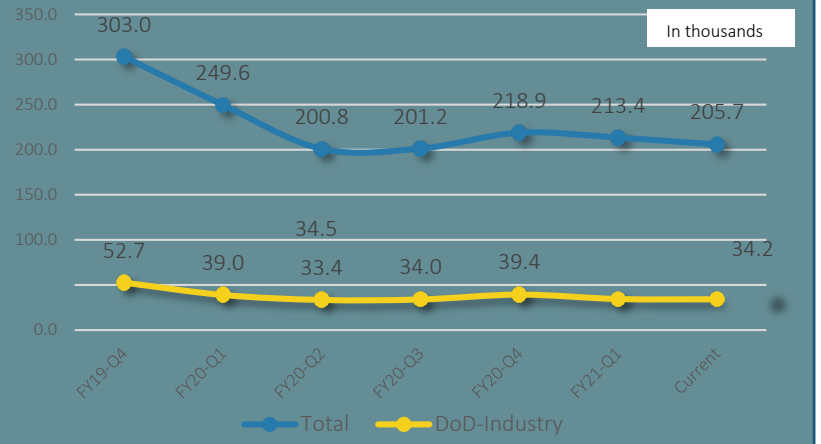
Industry Updates-April 2021

- **September Elections for 2 Industry Members**
- **Industry NISP Priorities/Watch List**
  - New NISPOM, 32 CFR, Part 117
  - TWF 2.0-Personnel Security Reform
  - Information Sharing
  - Operating under COVID and Return to Work
  - National Industry Security Program Systems
  - Controlled Unclassified Information (CUI)
- **Focus Areas**
  - Partnership/Stakeholders
  - Industry Engagements-Unity-Staying Informed
  - Focused Strategic Collective Priorities

DCSA PV INVESTIGATIONS/ADJUDICATIONS | *Industry*

INVESTIGATION

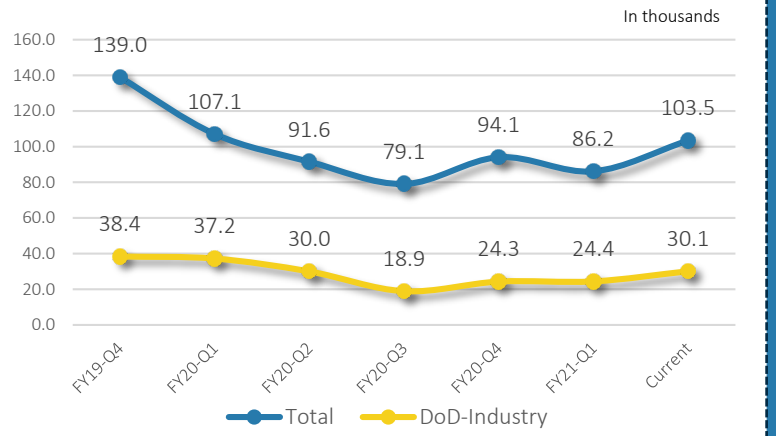
CURRENT INVENTORY	
All DCSA Customers	205.7K
Industry Only	34.2K



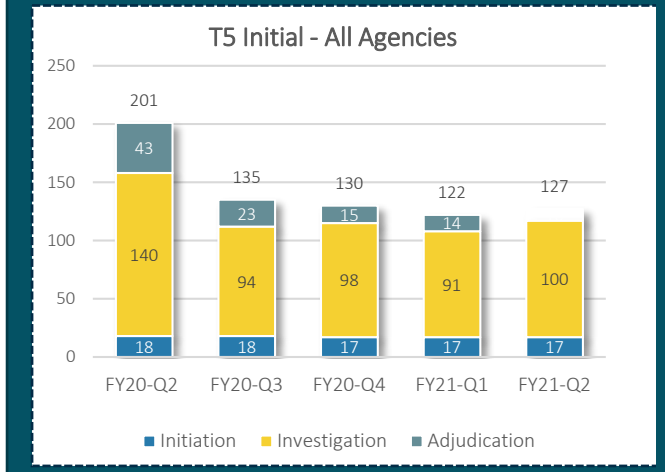
ADJUDICATION

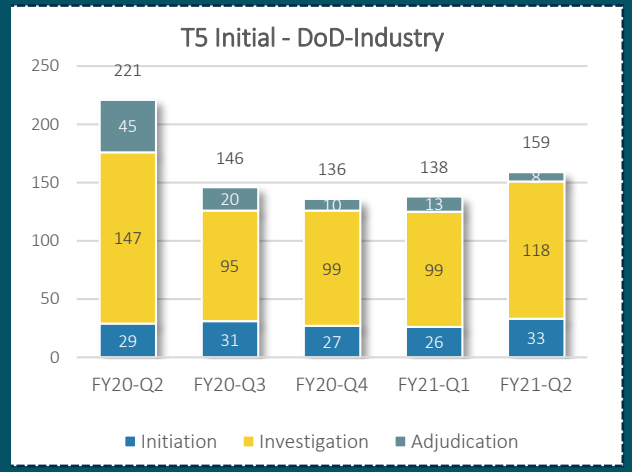
DoD CAF Only

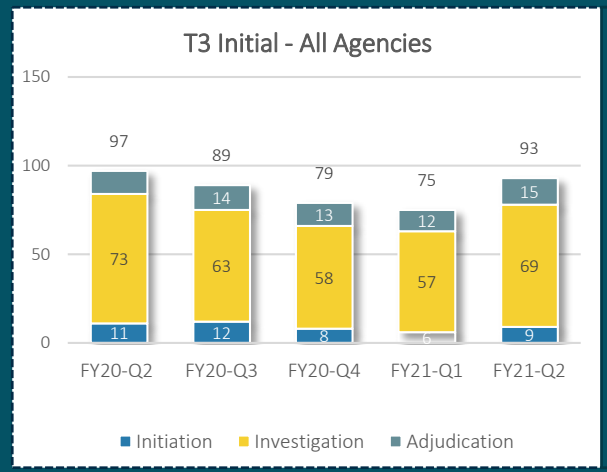
CURRENT INVENTORY	
CAF All	103.5K
Industry Only	30.1K

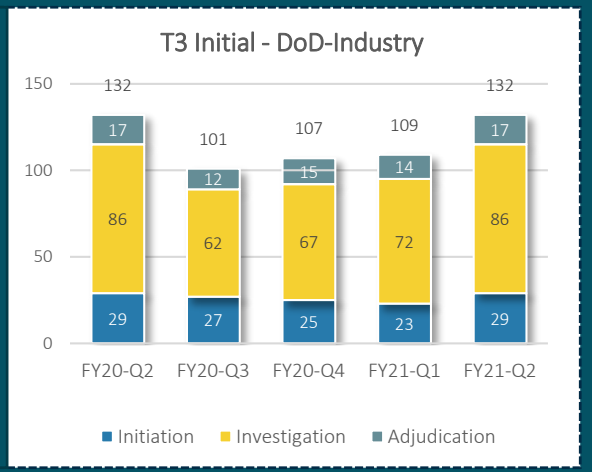


END-TO-END TIMELINESS (Fastest 90% of adjudicated investigations in days)









DCSA VROC – Industry Updates

FY21 PSI Execution

~1M
NISP Contractors With Clearance Eligibility

90k
Requests for Investigations Processed

4,700
Incidents Triaged

Continuous Evaluation

~675,000
Industry Subjects Enrolled in CE*

121,000
Industry PRs Deferred into CE to Date**

6%
Rate of CE Alerts Received

***Note**:*
** DoD CE Program TW 1.25 compliant*
*** Industry Deferred PRs are enrolled in TW 1.5 data sources to support reciprocity*

Early Detection

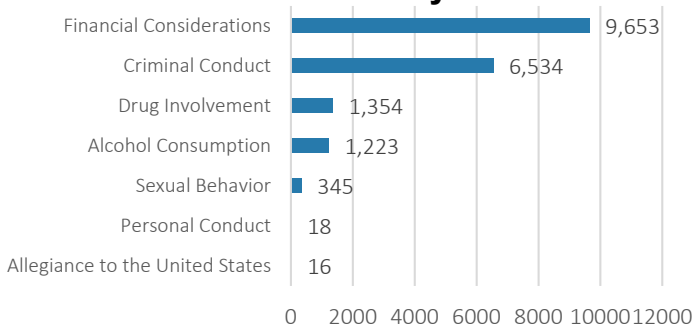
Early Detection and Risk Mitigation, before next PR due to begin

Secret: 7 Years 1 Month

Top Secret: 2 Years 7 Months

Industry CE Alert Data

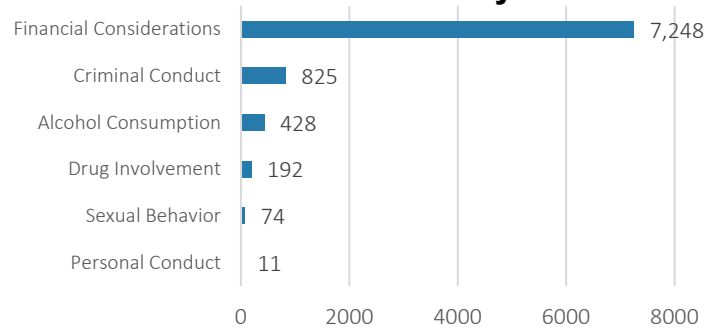
CE FY21 Valid Alert by Guideline



~19K
Valid Industry CE Alerts

~14K
Unique Industry Subject

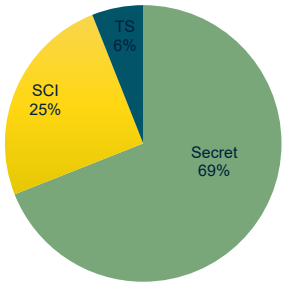
CE FY21 Actionable Alert by Guideline

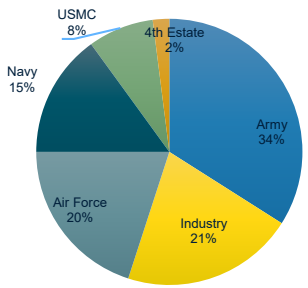


~8.7K
Actionable Industry CE Alerts

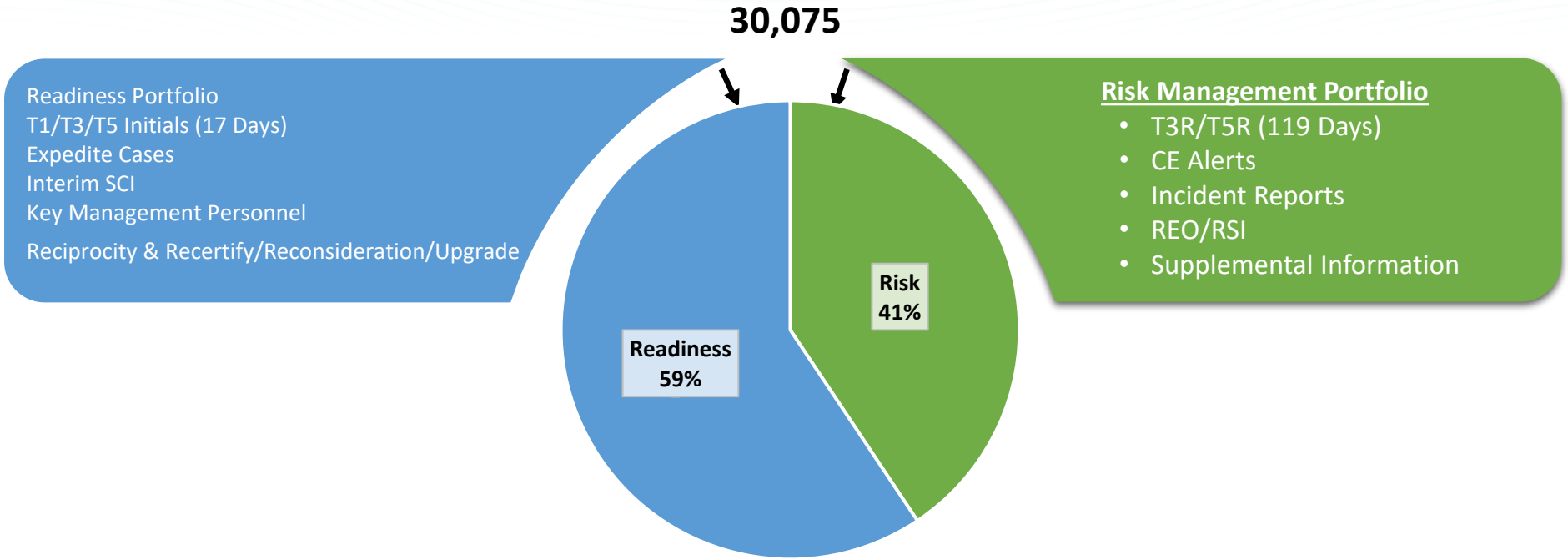
~8K
Unique Industry Subject

CE Population





DoD CAF Operational Update - Industry



FY21 Focus Areas

- DoD CAF continues Meeting Adjudicative Timeliness goals in FY21Q2 and expects to continue throughout FY21
- Maintain Healthy Inventory and execute national security eligibility, civilian suitability and credentialing decisions
- Improve Quality and Consistency of Adjudicative Decisions and business processes through workforce development and training
- Strengthen Relationships with personnel security partners
- Standardized Reciprocity Program within DCSA to improve program performance
- Destigmatize seeking Mental Health Care for cleared persons
- COVID-19. CAF Operating at Full Mission Capacity while maximizing telework

Metrics as of March 31, 2021

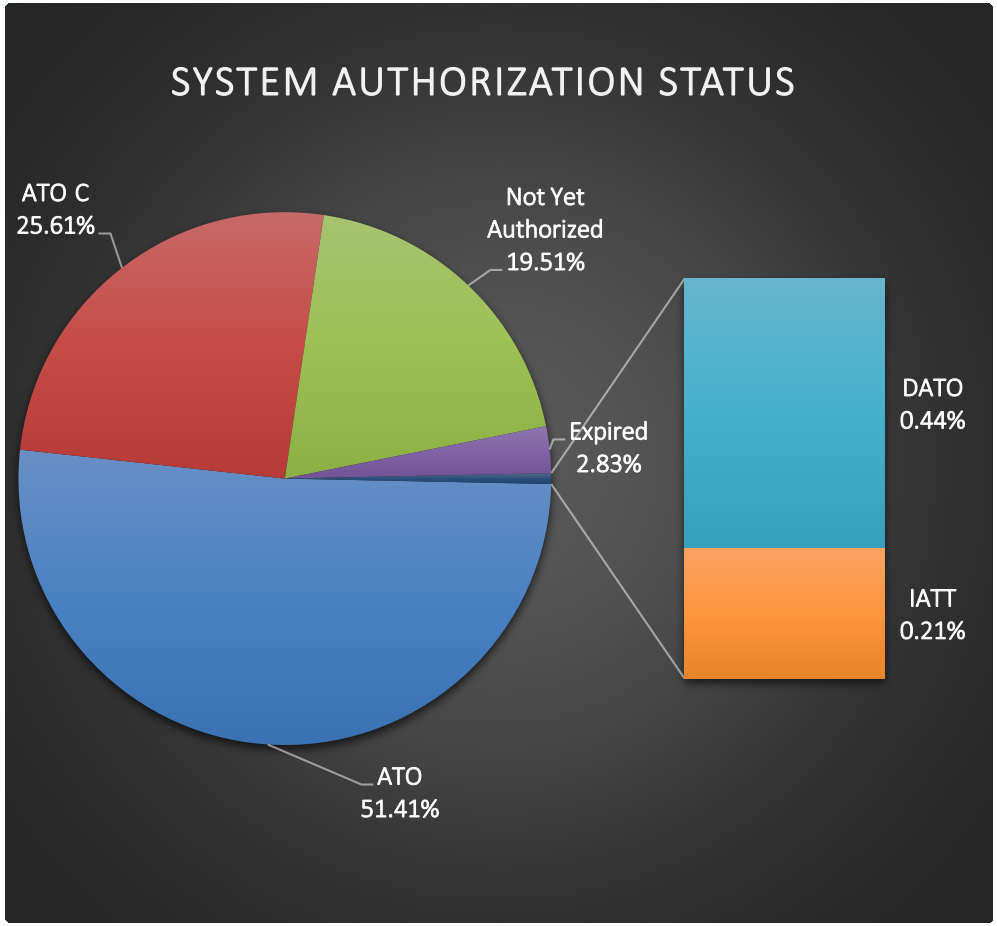
FY21 CAF Annual Report. https://www.dcsa.mil/Portals/91/Documents/DODCAF/resources/DCSA_FY20_CAF_Annual_Report_022421_Web.pdf.

DCSA
NISA WORKING GROUP
UPDATE

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

DAVID SCOTT
NISP AUTHORIZATION OFFICE
CRITICAL TECHNOLOGY PROTECTION

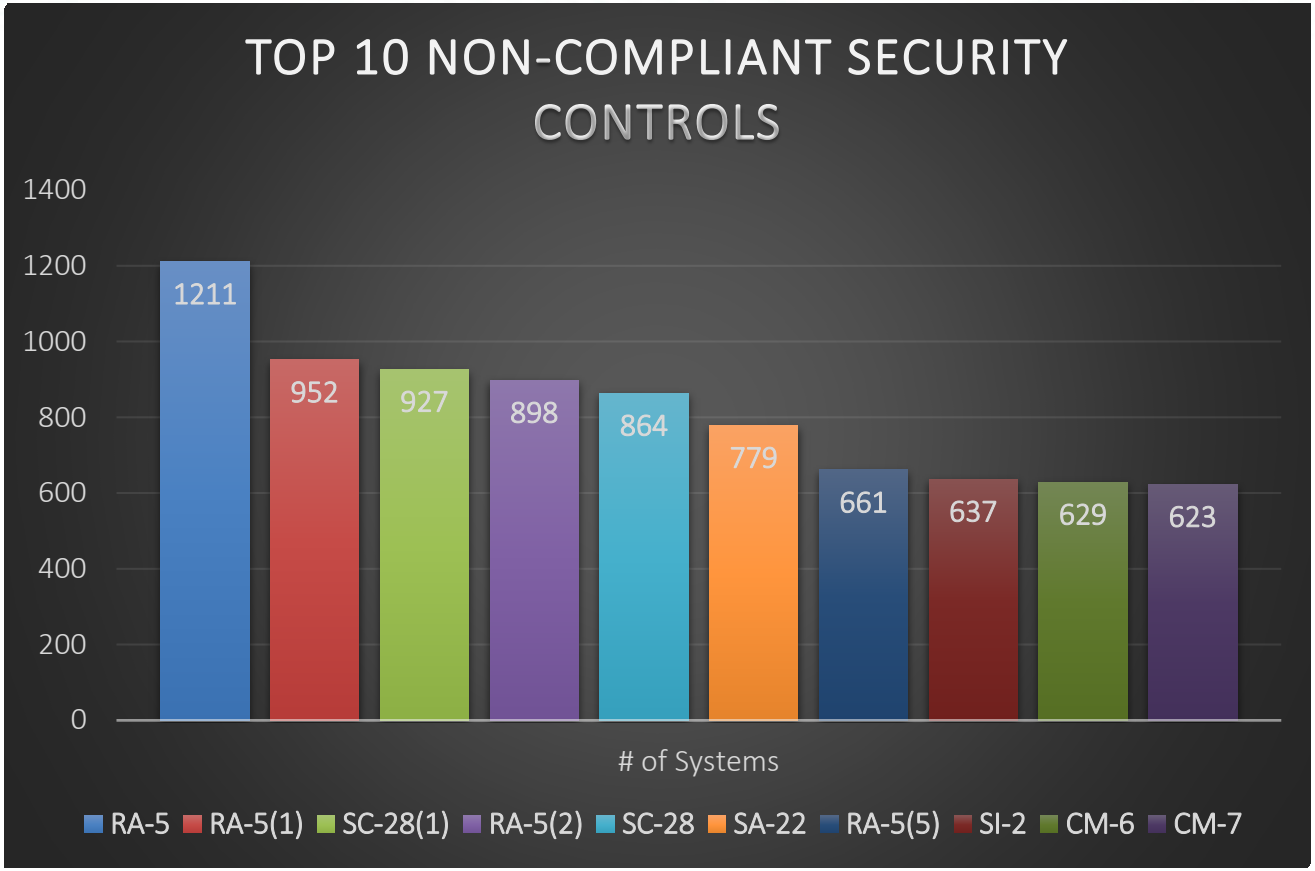
National Metrics



NISP eMASS Metric	Total
# Registered Systems in NISP eMASS	6,292
# of Authorizations Processed in FY21	2,995
# of NISP eMASS Users	3,649

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).

National Metrics



Security Control Information

RA-5: Vulnerability Scanning
RA-5(1): Vulnerability Scanning | Update Tool Capability
SC-28(1): Protection of Information at Rest | Cryptographic Protection
RA-5(2): Vulnerability Scanning | Update by Frequency / Prior to New Scan / When Identified
SC-28: Protection of Information at Rest
SA-22: Unsupported System Components
RA-5(5): Vulnerability Scanning | Privileged Access
SI-2: Flaw Remediation
CM-6: Configuration Settings
CM-7: Least Functionality

Overview: This slide provides the top 10 non-compliant security controls within the NISP. In addition, the number of systems with the identified non-compliant security control is listed. A security control is deemed non-compliant when it is not properly implemented, operating as intended, and/or producing the desired outcome with respect to meeting established security requirements.

DAAPM Update

- Future DAAPM Revision (TBD - 2022)
  - NIST SP 800-53 Revision 5
    - NAO is tracking the transition from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4 to Rev. 5.
    - Prior to updating the DAAPM, the updated Committee on National Security Systems Instruction (CNSSI) 1253 must be released.
  - An internal Working Group developing a Connection Process Guide (CPG) in order to assist all stakeholder with the establishment of interconnections. The CPG will provide process flows, templates, and guidance.

NISP eMASS Common Issues

1. Failing to follow the guidance in the NISP eMASS Industry Operation Guide
2. Incorrect System Name/System Acronym - *DCSA guidance for NISP eMASS system naming must be followed*
3. System details not fully populated
4. Incomplete System Description
5. Improper application of overlays
6. Artifacts needed to support authorization decision are not included in the security plan
7. Risk Assessment Reports (RAR) are not conducted at both the organization and system level. RARs must fully address: (1) relevant threats, (2) vulnerabilities (internal and external), (3) impacts to the organization, and (4) likelihood
8. Unsatisfactory inputs for Implementation Plan, SLCM, and Test Results (*All CCIs must be addressed*)
9. Plan of Action & Milestones (POA&M) is not accurate and/or does not address Non-Compliant security controls
10. Failing to submit security plan 90 days prior to Authorization Termination Date (ATD)

Questions

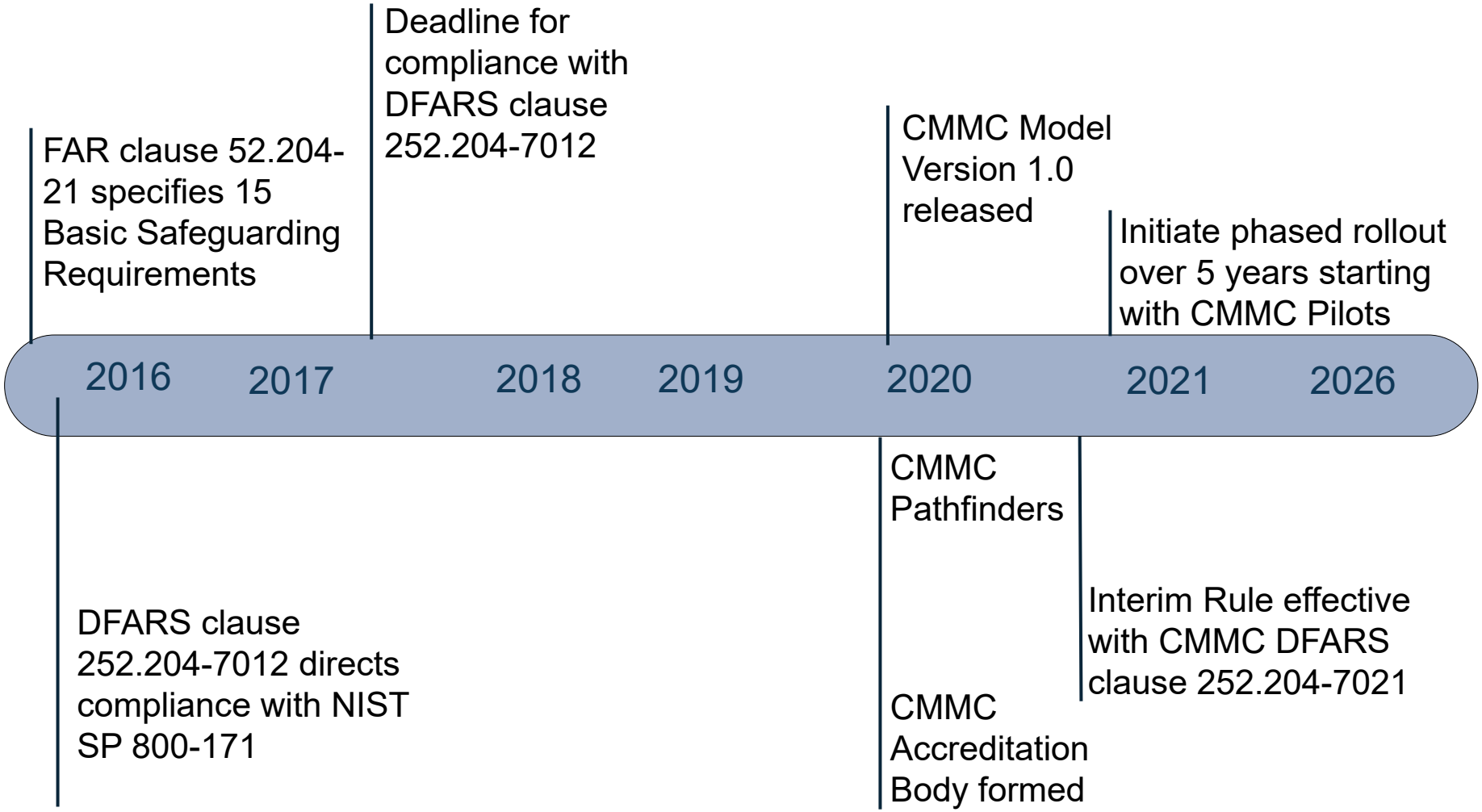
- Use available resources (DAAPM, eMASS [HELP], NISP eMASS Internal and Industry Operation Guide, and DISA RMF Functionality Guide).
- Visit the DCSA website: https://www.dcsa.mil/mc/ctp/

Securing the DoD Supply Chain

Cybersecurity Maturity Model Certification

Ms. Stacy S. Bostjanick
Acting Director of Supply Chain Risk Management

CMMC Regulatory and Implementation Timeline



DFARS Interim Rule for CMMC in effect; DoD initiating CMMC Pilot Kick Off meetings

DFARS Clause 252.204-7012: The Foundation for CMMC

CMMC complements DFARS clause 252.204-7012: Safeguarding Covered Defense Information [Controlled Unclassified Information (CUI)] and Cyber Incident Reporting

DFARS clause 252.204-7012 requires contractors/subcontractors to:

- Safeguard CUI by implementing cybersecurity requirements in NIST SP 800-171
  - Document in a System Security Plans (SSP) how requirements are implemented
  - Maintain a Plan of Action and Milestones (POAM) for unimplemented requirements
  - Obtain approval from Contracting Officers for any variances or "alternate but equally effective controls" implemented to meet the requirements
- Report cyber incidents (to include lost or stolen devices)*
- Isolate and submit malicious software for analysis*
- Facilitate damage assessments
- Flow down the clause to subcontractors if CUI is conveyed (not applicable to COTS)

Contractors and subcontractors self-attest to compliance

*DoD Cyber Crime Center (DC3)

DFARS Case 2019-D041
Assessing Contractor Implementation of Cybersecurity Requirements

The *interim rule* took effect 30 Nov 2020 / DoD implementing a 5-year phased roll-out

DFARS Provision 252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements	DFARS Clause 252.204-7020 NIST SP 800-171 DoD Assessment Requirements	DFARS Clause 252.204-7021 Cybersecurity Maturity Model Certification Requirements
Solicitation Notice: Basic Assessment Score required in SPRS for contract award • A NIST SP 800-171 DoD Assessment (Basic, Medium, High) summary level score must be posted into DoD's Suppliers Risk Performance System (SPRS) for the applicable CAGE code and Systems Security Plan • The summary level score must remain current (not older than 3 years unless a lesser time is specified) throughout the life of the contract, task or delivery order	**Basic Assessment Score required in SPRS to be considered for contract award** • Applicable to companies subject to DFARS clause 252.204-7012 • Post award, if DoD deems a Medium or High assessment is necessary due to program sensitivity, provide DoD access to facilities, systems and personnel • Include clause in all subcontracts or other contractual instruments including subcontracts for commercial items • Confirm subcontractor compliance with SPRS reporting if receiving CUI	**Cybersecurity Maturity Model Certification Required by contract award effective 1 Oct 2025** • Until 1 Oct 2025, OUSD(A&S) must approve clause in new acquisitions • Contractor certification level must be maintained for contract duration • Clause must be flowed down; primes must ensure subs are certified at required CMMC level prior to awarding subcontract

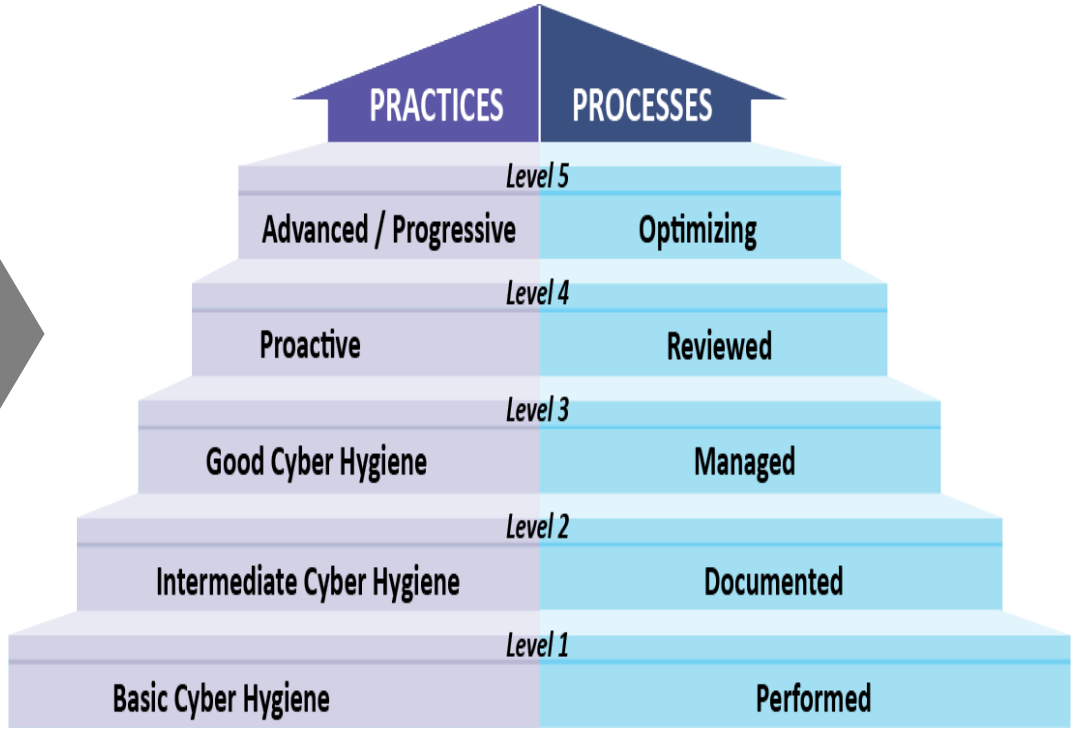
- Interim rule clauses are applicable to contracts, task orders and delivery orders
- Not applicable to micro-purchases or solicitations exclusively for the purchase of COTS products

CMMC Model Structure

17 Capability Domains (v1.0)

Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (SAS)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AA)	Personnel Security (PS)	System and Communications Protection (SCP)
Configuration Management (CM)	Physical Protection (PP)	System and Information Integrity (SII)
Identification and Authentication (IDA)	Recovery (RE)	

Capabilities are assessed for Practice and Process Maturity



CMMC Practice Progression

LEVEL 1
BASIC CYBER HYGIENE

17 PRACTICES

- ✓ Demonstrate compliance with Federal Acquisition Regulation (FAR) 48 CFR 52.204-21

LEVEL 2
INTERMEDIATE CYBER HYGIENE

72 PRACTICES

- ✓ Comply with the FAR
- ✓ Encompasses a select subset of 48 practices from the NIST SP 800-171
- ✓ Perform an additional 7 practices to support intermediate cyber hygiene

LEVEL 3
GOOD CYBER HYGIENE

130 PRACTICES

- ✓ Comply with the FAR
- ✓ Encompasses all practices from the NIST SP 800-171
- ✓ Perform an additional 20 practices to support good cyber hygiene

LEVEL 4
PROACTIVE

156 PRACTICES

- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 plus 20 additional practices
- ✓ Includes a select subset of 11 practices from Draft NIST SP 800-171B
- ✓ Perform an additional 15 practices to demonstrate a proactive cybersecurity program

LEVEL 5
ADVANCED / PROGRESSIVE

171 PRACTICES

- ✓ Comply with the FAR
- ✓ Encompasses all practices from the NIST SP 800-171 plus 20 additional practices
- ✓ Includes a select subset of 15 practices from Draft NIST SP 800-171B
- ✓ Includes an additional 26 practices to demonstrate an advanced cybersecurity program

Further reduces risk of advanced threats

CMMC Risk Reduction: Pathfinders

- **OUSD(A&S) funded risk reduction activities to inform CMMC implementation**

Missile Defense Agency (MDA) Pathfinder (Apr 2020 – present)

Activity: Mock Assessments
Mock Assessors trained by CMMC-AB
Conducted mock assessments:
- CMMC Level 3 'delta' of prime contractor
- CMMC Level 3 and Level 1 of two subcontractors

Objective
Validate drafted CMMC Assessment Guides and gather lessons learned

Outcome
Identified Lessons Learned to improve draft documentation and assessment processes

Activity: Acquisition Tabletop
Conducted a sequence of evolving TTXs that focus on the DoD's acquisition processes from RFI to post contract award.

Objective
Identify and reduce risks associated with implementing CMMC in future acquisitions

Outcome
Developed exemplar RFI, RFP and flow down language to support contract actions

Defense Logistics Agency (DLA) Pathfinder (Sep 2020-Present)

Planned Activity: Mock Assessments
Conduct two mock assessments:
- CMMC Level 3 of two prime contractors
- Assessed by authorized C3PAOs

Objective
Identify and reduce risks associated with newly authorized C3PAOs

Mock Assessments are non-attributional, non-punitive and do not result in a certification

CMMC Implementation: Pilots (2 of 2)

- The following candidate programs have been identified by Services and Agencies:

Service or Agency	Program
Army	Foreign Military Sales (FMS) Field Service Representative Support
	Woman, Infant, & Children (WIC) Overseas Program for DHA-J10-TRICARE
	Main Operating Base-Installation Service Nodes (MOB-ISN)
Navy	Integrated Common Processor
	F/A-18E/F Full Mod of SBAR & Shut off Valve
	DDG-51 Lead Yard Services / Follow Yard Services
Air Force	Mobility Air Force Tactical Data Links
	Consolidated Broadband Global Network Area Network Follow-On
	Azure Cloud Solution
Missile Defense Agency	Technical Advisory and Assistance Contract

- DoD plans to implement CMMC using a phased rollout over five years commencing with a target of up to 15 new acquisitions in FY21:
  - The rollout ramps up over 5 years with CMMC in up to 475 new prime contracts by FY25
  - Until 1 Oct 2025, OUSD(A&S)/OCISO(A&S) CMMC Office must approve the use of the clause for new acquisitions

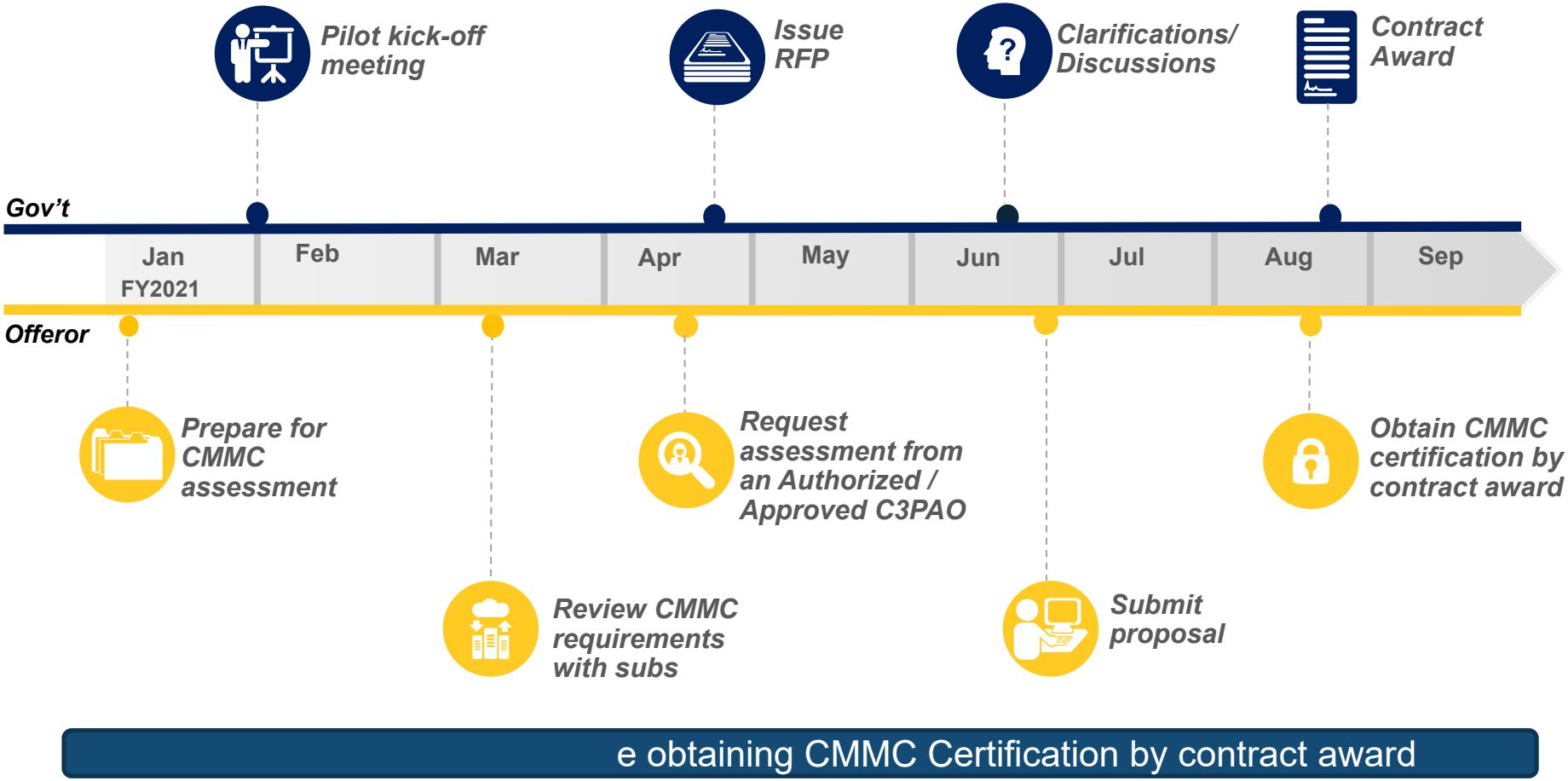
DIB Contractor / C3PAO Business Relationship
Basic CMMC Process

*DIB Contractor is AKA: "OSC – Organization Seeking Certification
**C3PAO – CMMC Third Party Assessment Organization

Notional CMMC Pilot Timeline

KEY PILOT MILESTONES

Below is a notional CMMC Pilot timeline outlining key milestones for the government and offerors:



Pilot Key Takeaways

Until 1 Oct 2025, CMMC requirements will only be included in new acquisitions with the approval of OUSD(A&S) / OCISO(A&S)

CMMC Pilot programs will include applicable CMMC requirements in RFPs

- OUSD(A&S) is not funding CMMC Pilots
- CMMC certification must be met by contract award
- CMMC certification is required of the enterprise network or particular segment where FCI or CUI is processed, stored, or transmitted in performance of the particular contract
- CMMC certification must be maintained for the duration of the contract; recertification may be necessary depending on expiration date of the CMMC certification versus the contract end date

CMMC Pilot contractors will be required to achieve CMMC Certification

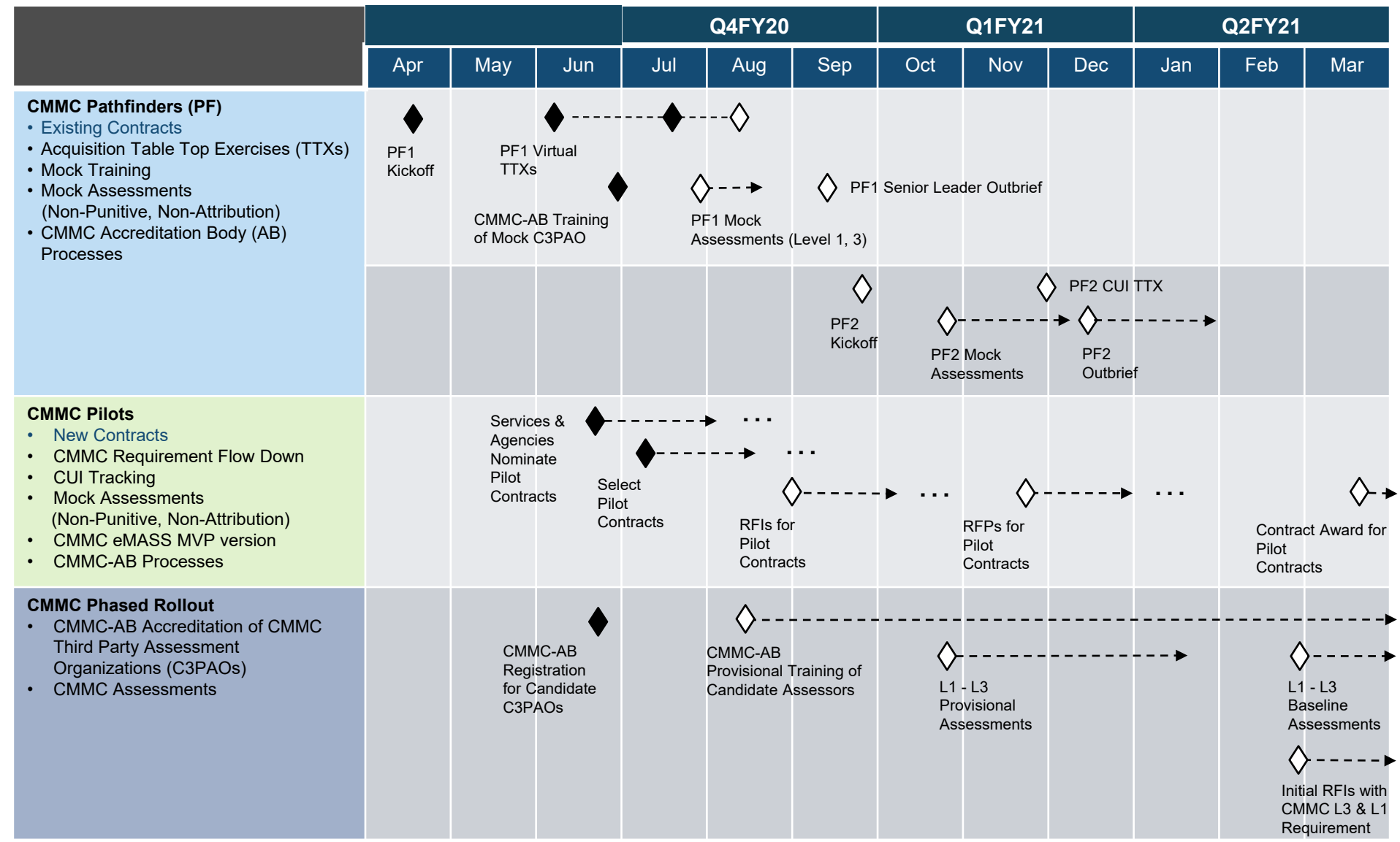
- DIB Contractor enters into Business Relationship with an authorized / approved C3PAO
- CMMC certification is achieved by passing a CMMC assessment conducted by C3PAO
- All CMMC practices and processes must be implemented at the required CMMC Level
- CMMC does not allow POAMs
- If there are assessment findings, the contractor will need to remediate to achieve CMMC certification
- CMMC Certification is good for three years

OUSD(A&S) will provide guidance and support during Pilot roll-outs

Updated on 20 Jul 2020

UNCLASSIFIED

Draft CMMC Schedule



Projected CMMC Roll-Out

- **OUSD(A&S) will work with Services and Agencies to identify candidate programs that will have the CMMC requirement during FY21-FY25 phased roll-out**

Total Number of Contracts with CMMC Requirement				
FY21	FY22	FY23	FY24	FY25
15	75	250	479	479

	Total Number of Prime Contractors and Sub-Contractors with CMMC Requirement				
	FY21	FY22	FY23	FY24	FY25
Level 1	895	4,490	14,981	28,714	28,709
Level 2	149	748	2,497	4,786	4,785
Level 3	448	2,245	7,490	14,357	14,355
Level 4	4	8	16	24	28
Level 5	4	8	16	24	28
Total	1,500	7,500	25,000	47,905	47,905

- **All new DoD contracts will contain the CMMC requirement starting in FY26**

https://www.acq.osd.mil/cmmc/index.html

General Services Administration

- Removal of GSA Approved Black Label
- Containers & Vault Doors

- NISPAC meeting 4/14/2021

General Services Administration
Interagency Committee on Security Equipment and Locking Systems
27 January 2021

To: All GSA-Approved Manufacturers & Training Organizations

Subject: Phase-out Plan for Black Label Security Containers & Vault Doors

All,

The General Services Administration, Interagency Committee on Security Equipment (GSA/IACSE) in coordination with the Information Security Oversight Office (ISOO) is developing a phase-out plan for all GSA-approved security containers and vault doors manufactured prior to 1989 (Black GSA Label). The plan will rescind the approval for all GSA-approved security cabinets and vault doors manufactured from 1954 through 1989 (Black GSA-Approval labels) to store classified information and materials over a period of 4 years starting on as of October 1, 2024

The phase-out plan will start with the oldest cabinets (class 2) and proceed to the last of the Black Label security equipment (class 5 & 6) over a period of at least 4 years as outlined below.

All GSA-approved Class 1, 2, 3 & 4 cabinets manufactured under Federal Specifications AA-F-357 and AA-F-358 600 (Revision Indicators A - F) will be considered obsolete for the storage of classified information and materials as outlined in the below chart.

All GSA-approved Class 5 & 6 cabinets and vault doors manufactured under Federal Specification AA-F-358 (Revision Indicators A - F) and AA-D-600 (Revision Indicators A - C) before 1989 will be considered obsolete for the storage of classified information and materials as of 1 October 2028.

Black Label Phased-Out Plan Chart

GSA CLASS	FED SPEC	REVISION	YEARS PRODUCED	YEARS OF SERVICE	END OF SERVICE
1	AA-F-357	A - F	1968 - 1982	46 - 60	1 October 2028
2	AA-F-357	A - F	1954 - 1970	50 - 70	1 October 2024
3	AA-F-358	A - F	1956 - 1968	52 - 69	1 October 2025
4	AA-F-358	A - F	1956 - 1968	52 - 69	1 October 2025
5	AA-F-358	A - F	1968 - 1989	31 - 60	1 October 2028
5	AA-F-363	A - B	1963 - 1989	57 - 65	1 October 2028
5	AA-D-600	A - B	1963 - 1989	57 - 65	1 October 2028
6	AA-D-600	A - C	1963 - 1989	57 - 65	1 October 2028
6	AA-F-358	A - F	1968 - 1989	52 - 60	1 October 2028

Please contact the Chairman of the GSA/IACSE, Mr. Christopher Pollok, if you have and questions at Christopher.pollock@gsa.gov.

Sincerely,

DocuSigned by:
Christopher Pollock
46435F98A6014E3...

Christopher Pollock
Chairman
Interagency Committee for Security Equipment (IACSE)
General Services Administration
1800 F Street, NW
Washington, DC 20405

Sincerely,

JUSINO.ROY.1009641080
Digitally signed by JUSINO.ROY.1009641080
Date: 2021.01.27 16:09:01 -08'00'

Roy Jusino
Chairman
Security Equipment and Locking Systems (SEALS) Sub-committee
NAVFAC EXWC
1100 23RD Avenue
Port Hueneme, CA 93043-4370

Examples

RED Label Class 6
GSA-approved
Container

BLACK Label Class 3
GSA-approved
Container

Why?

- Black Label GSA containers can be 30 - 65 years old which leads to:
  - Safety Issues
    - Drawer slides worn out
    - Drawer stops breaking off
    - Rusty interiors
  - Security Issues
    - Old steel plate designs (no lock box)
    - Old hard plate designs (cast lock box)
    - Old combination locks (mechanical)
  - Repair Issues
    - No parts available
    - Manufacturers are no longer in business

Industry Requirements

- Survey your facilities for GSA-approved containers
    - Determine how many old Black Label containers and vault doors are still in use
    - Determine if they are still required
        - Facility accreditation review
        - Possible classified Holding's reduction
- Work with your Accrediting Authority and/or Contracting Officer to formulate a Company plan for replacement of the identified Black Label containers & vault doors that are still required over the allotted time period.

Questions?

Thank You!

Information Security Oversight Office

Protect • Inform • Assess

NISPPAC Working Groups

- NISP Information Systems Authorization (NISA)
  - Discussed Solid State Sanitization
  - Last mtg 3/31/2021
- Clearance
  - NISPOM rule effective 2/24/2021
    - Contractors have to comply no later than 8/24/2021
    - Format is different
  - Last mtg 3/3/2021

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

- 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