



## **National Industrial Security Program Policy Advisory Committee (NISPPAC) Public Meeting Report for the 74<sup>th</sup> Meeting**

**Wednesday, May 28, 2025 (10am-1pm ET)  
National Archives and Records Administration (NARA)  
Information Security Oversight Office (ISOO)  
Meeting held in the McGowan Theater and Virtually**

### **Minutes**

*The meeting was called to order at 10:00am ET*

#### **NISPPAC Chairman Remarks**

- Michael Thomas, NISPPAC Chairman and Director of the Information Security Oversight Office (ISOO), called the meeting to order and delivered opening remarks.
- ISOO, as the convening authority, is spearheading an effort to capture NISP recommendations for the President in accordance with Executive Order (EO) 12829.

#### **Administrative Matters**

- Jennifer May, NISPPAC Alternate Designated Federal Officer (ADFO), briefed on administrative matters.
- Membership changes: Natasha Sumter and Tracy Kindle departed as the NISPPAC members from the Department of Energy (DOE). They were replaced by Jaime Gordon (Primary), Monica Marks (Alternate), and Theodore Banks (Alternate). Della Morrison, NISPPAC member from the National Security Agency (NSA) retired. A primary NISPPAC member has not yet been named. Blane Vucchi continues to serve as the alternate member. Jason Steinhour replaced Robin Nickel as the alternate NISPPAC member from the Department of the Navy. James McAlary replaced Elizabeth O’Kane as the primary NISPPAC member for the Department of the Army. Jennifer May, ADFO is being replaced by Benjamin Rogers.
- Michael Thomas adjourned the meeting at 1:26pm ET.
- The previous meeting, held on November 13, 2025, had its minutes certified to be true and correct by Mr. Thomas on January 24, 2025. They were posted to <https://www.archives.gov/isoo/oversight-groups/nisppac/committee.html> on February 4, 2025.

- Action items still open from the last meeting:
  - The Department of Defense (DoD) asked ISOO to assist in engaging with the Small Business Administration regarding military departments' ability to meet small business requirements. This item is still pending with ISOO.
- Action items closed from the last meeting:
  - The first item of interest is the status of the Executive Branch's Controlled Unclassified Information (CUI) study. The National Security Council (NSC) began to review the Classified National Security Information (CNSI) and CUI Executive Orders in 2022. CUI Notice 2022-01 is the last formal guidance we provided regarding the status of that process and the program. ISOO is still awaiting further guidance from the new administration's NSC regarding its plans in the information management space as they pertain CNSI, CUI, and Special Access Programs (SAP). In the meantime, ISOO continues to fulfill their responsibilities under the existing policy framework that governs the CNSI and CUI systems.
  - DoD expressed its intent to invite the project lead for Cybersecurity Maturity Model Certification (CMMC) from the DoD Chief Information Officer (CIO) to provide a program update at the next public meeting of the NISPPAC. Stacy Bostjanick briefed during the public meeting.
  - DoD invited Jill Baker to speak at the next public meeting of the NISPPAC on National Background Investigation Services (NBIS). While Jill Baker did not brief during the public meeting, Jeff Spinnanger answered questions about NBIS from a policy perspective.
  - DoD provided an update on the status of the NISPOM.
  - The Office of the Director of National Intelligence (ODNI) provided a Threat and Operational Risk Information System (TORIS) update.
  - The Defense Counterintelligence and Security Agency (DCSA) continued to work on guidance and training for the SF-328, "Certificate Pertaining to Foreign Interests."
  - DCSA provided a demo of the personnel vetting questionnaire in NBIS to the Industry NISPPAC members.
  - The Central Intelligence Agency (CIA) provided Industry insight in their FOCI vetting process.
  - DOE addressed how often they perform business assessments.

- Mr. Thomas opened voting on the proposed changes to the NISPPAC bylaws. They were passed by a unanimous vote and were amended effective immediately.

## **Industry Update**

- Isaiah Rivers, NISPPAC Industry Spokesperson, delivered the update.
- The collaboration and partnership between Government and Industry was on display in the quick response to issues identified during the recent NBIS update rollout.
- Gregory Sadler and David Tender will be departing as NISPPAC Industry members. Industry will be holding elections in August to identify replacements. Christopher Stolkey is the newest NISPPAC Industry member. Christy Wilder is the new Industry Representative to the NISPPAC for the Professional Services Council (PSC).
- Industry requested that ISOO convene a meeting of the Cognizant Security Agencies (CSAs) to discuss CUI. Inconsistency and incongruency in CUI programs and guidance by Federal agencies negatively impacts Industry. As the conversation progresses, Industry would like to be included in the discussion.
  - *DoD agreed to participate during their remarks.*
  - *The Department of Homeland Security (DHS) agreed to participate during their remarks.*
- Industry would like to understand the communication channels CSAs utilize to communicate messages to Industry.
  - *DCSA has multiple avenues to communicate with Industry, including meetings such as the NISPPAC, DCSA website, DCSA social media, and other speaking engagements with Industry audiences.*
  - *DHS stated that they share information with Industry in numerous ways, including Information Sharing and Analysis Centers (ISACs), DHS alerts notifications, DHS online platforms and portals, and DHS Industry focus groups.*
  - *DOE stated they have multiple policy panels, working groups, and various information resource platforms where Industry can find relevant information. DOE encouraged Industry personnel to reach out if they would like to be added to a policy panel or working group.*
- Industry would like to discuss reciprocity of training with the government.
  - *DHS stated that they accept Intelligence Community (IC) partner training and DCSA collateral training.*

- *ODNI agreed to organize discussion within the IC on reciprocity of training.*
- *CIA accepts other IC elements' training, except when an individual has access to CIA high-side systems. In that instance, all training must be done on CIA systems.*
- Gregory Sadler, Industry, continued with the Industry update discussing CUI. He noted inconsistencies in CUI guidance, internally within DoD and especially in the Request for Proposal (RFP) space. While it is important that there is a discussion regarding CUI across the CSAs, CSAs also need to have internal conversation regarding CUI.
  - *DoD acknowledged the need to standardize CUI guidance across the department and is willing to meet with other CSAs to discuss CUI.*
  - *DHS is willing to meet with other CSAs to discuss CUI.*
- LaToya Coleman, Industry, asked about Sensitive Compartmented Information (SCI) indoctrination authority for Industry. Because Industry is unable to conduct SCI briefings for some of the military departments, which delays getting personnel in program. Industry is asking DoD to work with the service agencies to expand the SCI indoctrination authority and to continue to review the nomination process. Industry would also like to have additional meetings with DoD and the service departments to come up with a better process moving forward.
- Chris Stolkey, Industry, highlighted the lack of sanitization procedures for solid state drives. This becomes an issue when solid state drives are involved in a spill and can cost millions of dollars. Industry wants to work with the government in solving this problem.
- LaToya Coleman, Industry, requested engagement with DoD within the next 30 days regarding Industry requirements and feedback on NBIS. Industry would like these engagements to continue until successful deployment of NBIS and any other concurrent system or application going forward.
  - *DOD agreed to engage on this topic.*
- Charlie Sowell, Industry, noted that Industry has received very little guidance regarding the EOs signed by the administration since January. Industry requested that ISOO coordinate with the CSAs to provide guidance to Industry as soon as possible on all EOs relevant to the NISP.
  - *ODNI expects to announce the re-issuance of several Trusted Workforce 2.0 (TW 2.0) policies and artifacts in response to about a half dozen EOs. ODNI noted that many of these updates have no impact on Industry.*



- LaToya Coleman, Industry, asked DCSA to address what the findings were from the DCSA tiger team tasked with reducing the investigation timelines, what is being done to address the findings, and what Industry should expect moving forward.
  - *DCSA has not seen an increase in timelines since last year. DCSA has reduced background investigation inventory from 290,000 in September 2024 to 222,000 in May 2025. In April, DCSA witnessed timeliness improve 10%.*
  - *DCSA is using a data-driven approach to make changes that will have an enduring impact on business processes. DCSA anticipated continued improvement in performance numbers, even while reducing the workforce through various workforce shaping methods.*
- LaToya Coleman, Industry, asked ODNI to explain the SCI processing timeline and address what ODNI is doing to help reduce the timeline. Industry would also like ODNI to create a working group, with Industry participation, to help reduce the timeline.
  - *ODNI agreed to follow-up with LaToya on the request and gather details from Industry perspective to better inform working group participation.*
- LaToya Coleman, Industry, asked DCSA and DOD to partner with Industry in a working group on the Personnel Vetting Questionnaire (PVQ) to ensure a smooth transition.
  - *DCSA plans to roll-out the next phase of the PVQ to a limited audience in June 2025 and will engage with Industry to test the capability.*
- Gregory Sadler, Industry, requested that government inform Industry of any budgetary or personnel changes that will impact Authorizations to Operate (ATOs).
- Jane Dinkel, Industry, asked DCSA to break down the facility clearance lifecycle, identify timeline goals for each stage, and explain the recourse if DCSA does not meet timeline goals.
  - *DCSA stated that they have reduced facility clearance timelines while increasing outreach and efficiency. Last October, DCSA launched the security rating scorecard, which was developed in partnership with Industry. Those results so far indicate more fairness in scoring, and an overall improvement in security review ratings.*
  - *The current FCL inventory is less than 300 cases. DCSA has increased issuance of FCLs by 32% compared to last year.*
- Jane Dinkel, Industry, asked DCSA to provide a status update on the facility clearance orientation handbook. Industry provided input to DCSA for the creation of the handbook, but has not heard anything since that time.

- Jane Dinkel, Industry, noted inconsistencies in DCSA staff training at field locations and at the DCSA knowledge center. Recommendations and observations during inspections are mistakenly interpreted as requirements by investigators and answers provided by the knowledge center are inconsistent. Industry would appreciate uniform training across the field.
  - *The DCSA Security Academy was launched in October 2024. The academy will graduate the first cohort of students from the industrial security program in August 2025.*
  - *Just a few weeks ago, the academy launched a new curriculum for information system security professionals. These courses will help ensure that DCSA continues to perform at a high level with standard review processes across the board.*
- LaToya Coleman, Industry, asked ODNI for an update on the covered insider threat information sharing policy and the overhead billets policy.
  - *Regarding covered insider threat information sharing, ODNI stated the draft policy is being reworked to better address Congress's requirement and is in ODNI internal coordination.*
  - *Regarding the overhead billets policy, ODNI stated that the policy draft is in coordination with ODNI general counsel. ODNI will inform LaToya of an expected timeline at a later time.*
- Kathy Andrews, Industry, delivered an update on the physical security working group. The working group enjoys a strong relationship with the IC.
- Kathy Andrews, Industry, asked for standardization of key compliance dates for Special Access Program Facilities (SAPFs), especially from the military departments.
- Kathy Andrews, Industry, proposed a process for TEMPEST self-certification by Certified TEMPEST Technical Authorities (CTTAs).
  - *CIA advised that they do not conduct CTTA testing. However, if the spaces are built to the standards that CIA provides, then CIA will provide an accreditation without the testing. CIA does not need companies to pay for or conduct their own testing.*

### **DoD Update**

- Jeff Spinnanger, Director, Information and Acquisition Protection, Office of the Under Secretary of Defense for Intelligence & Security (OUSDI&S), delivered the update for DoD.

- DoD commended Industry for quickly alerting the government to problems experienced with NBIS.
- DoD is focused on data interoperability to ensure that classified and sensitive information can move securely and efficiently across the industrial base.
- DoD recognized the need for standardized security protocols and data formats. DoD is prioritizing policies that encourage scalable, standards-based solutions that drive interoperability and risk management, which includes an emphasis on secure cloud.
- DoD is piloting use of commercial providers to deliver classified spaces and networks.
- DoD agreed to participate in a CSA working group on CUI as Industry requested. DoD noted that Artificial Intelligence (AI) enables the adversary to more quickly aggregate seemingly harmless data, to include CUI, into powerful threat vectors.

### **DCSA Update**

- David Cattler, Director, delivered the update for DCSA.
- DCSA issued a strategic plan in March 2025 with an emphasis on three areas: moving DCSA to full performance and integration in each mission; anticipate and prepare for the future by equipping the agency to confront an evolving threat environment in the year 2040; and raise the level of understanding and awareness of DCSA as the premier provider of integrated security services for the federal government.
- DCSA got approval from DoD to move the NBIS software development program back into the execution phase of the DoD adaptive acquisition framework.
- In March 2025, DCSA met the first milestone on the product roadmap with the release of the initial iteration of the personnel vetting questionnaire for non-DCSA investigative service providers.
- In October 2024, DCSA launched the security rating scorecard. Results so far have indicated more fairness in scoring, and an overall improvement in security review ratings.
- DCSA is on track to complete 45 Cyber Operational Readiness Assessments (CORAs) in Fiscal Year (FY) 2025. DCSA plans to complete 60 CORAs in FY26.
- DCSA has noted an impressive increase in the quality of suspicious contact reporting coming from Industry and from academia.

### **Comments on DCSA Update**

- LaToya Coleman, Industry, asked DCSA about communication channels they intend to use to communicate with Industry.

- *DCSA stated they will utilize NISPPAC meetings, DCSA website, DCSA social media, and other speaking engagements with Industry audiences.*
- Jane Dinkel, Industry, asked when Industry will see guidance on the extension of the timeline to complete the SF-328. Jane noted that, at the last NISPPAC public meeting in November, DCSA agreed to extend the timeline for completing an SF-328 to six months, due to the significant changes to the form. However, now that the new SF-328 is live, Industry has not seen any guidance indicating an extension in the timeline.
- *DCSA stated they are looking forward to utilizing the NISPPAC and partnering with Industry on rebaselining what the SF-328 is and around communications.*

### **ODNI Update**

- Lisa Perez, Chief, Policy and Collaboration Group, Special Security Directorate, National Counterintelligence and Security Center (NCSC), ODNI, delivered the update.
- ODNI is planning to conduct a comprehensive review of Security Executive Agent Directive (SEAD) 4. This is based on feedback received in recent years.
- ODNI continues to work with the Office of Personnel Management (OPM), Office of Management and Budget (OMB), and DoD on Trusted Workforce 2.0 personnel vetting requirements.
- ODNI continues to work on updates to Scattered Castles and TORIS.
- Tessa Dutko, Physical and Technical Security Policy Officer, Center for Security Evaluation, NCSC, ODNI, provided an update on Intelligence Community Directive (ICD) 705.
- ODNI is working to get Sensitive Compartmented Information Facilities (SCIFs) up to compliance with current standards.
- In consultation with Industry, ODNI is looking to upgrade the entire 705 series of policy.
- ODNI plans to revise all 14 chapters of the technical specifications on SCIFs.

### **Comments on ODNI Update**

- Ike Rivers, Industry, asked, regarding the covered insider threat policy, if Industry is going to have the ability to be part of the process?
  - *ODNI stated they did not receive a response on this topic, but ODNI agreed to follow-up on this topic.*

## **CIA Update**

- Don, Chief, Office of Security Policy, provided the update for CIA.
- CIA's supply chain and acquisition assessment branch is responsible for vetting companies as part of the FOCI. Documentation that has to be submitted by relevant companies is used to supplement other available information and is closely evaluated to determine whether any foreign ownership exists within an entity or within its organizational structure.
- As of February 2025, all individuals must be tied to an active contract.
- Jennifer Alworth, Chief, Industrial Security Support Division, provided an update on CTTA testing.
- CIA will provide CTTA accreditation without the testing if spaces are built to CIA standards.
- CIA does not need companies paying for or conducting their own testing.

## **DHS Update**

- Richard Dejausserand, Deputy Director, Office of the Chief Security Officer (CSO), National Security Services Division, DHS, provided the update for the DHS.
- DHS stated they have not fully implemented CUI, however, DHS is willing to participate in a discussion with other CSAs on CUI. DHS has been working with DOJ on 12 different law enforcement related CUI categories.

## **Comments on DHS Update**

- LaToya Coleman, Industry, asked if DHS is waiting on the CUI EO to be released to fully implement a CUI program.
  - *DHS stated that is correct.*
- LaToya Coleman, Industry, asked for a meeting with the Chief Security Officer of DHS.
  - *DHS agreed.*
- Gregory Sadler, Industry, asked if DHS accepts DCSA collateral training in addition to IC partner training.
  - *DHS stated that they do accept DCSA collateral training.*

### **DOE Update**

- Jaime Gordon, Office of Security Policy, Program Planning & Management, delivered the update.
- In response to a question about DOE business assessments, DOE stated that their analysis is conducted through eFOCI, which is DOE's system of record. Business assessments are typically performed on a case-by-case basis.
- DOE encouraged Industry to reach out if there are questions regarding a specific business assessment.
- DOE highlighted the communication channels they utilize to connect with Industry and advised Industry to reach out if they want to participate in policy panels or working groups.

### **Nuclear Regulatory Commission (NRC) Update**

- Christoph Heilig, Chief, Personnel Security (PERSEC), provided the update for the NRC, but had no comments.

### **DOE Vetting Metrics Update**

- Monica Marks delivered the update.
- DOE met or exceeded investigation and adjudication goals for the last two quarters.

### **NRC Vetting Metrics Update**

- Christoph Heilig, PERSEC Chief, delivered the update.
- Except for Quarter 2 of FY24, NRC has met or exceeded goals in every quarter for the last 2 years.

### **DCSA NISP Cyber Security (NCSO) Update**

- David Scott, Deputy Assistant Director, NCSO/Authorizing Official (AO) delivered the update.
- DCSA is working toward centralized management of their memorandum of understanding (MOU) process.
- DCSA is currently defining all National Institute of Standards and Technology (NIST) Revision 5 requirements. DCSA expects to self-assess progress in the fall of 2025 and

partner with the NISP Information System Authorization (NISA) working group on the way forward.

### **Comments on DCSA NCSO Update**

- Gregory Sadler, Industry, asked about a timeline for release of the DCSA Assessment Authorization Guide (DAAG). Greg noted that Industry reviewed and provided feedback on the DAAG almost two years ago and there has not been a finalized and released version.
  - *DoD stated they anticipate the DAAG to be released by the end of July 2025.*

### **DCSA Adjudication and Vetting Services (AVS) Update**

- Donna McLeod, Senior Policy Advisor, PERSEC, delivered the update.
- DCSA case inventory has decreased nearly every week in 2025. The current volume is 222,000 cases.
- DCSA continues to work with the FBI regarding name checks. FBI name checks have slowed the process for DCSA.
- DCSA has benefited from early adoption of TW 2.0.

### **Comments on DCSA AVS**

- Gregory Sadler, Industry, asked if the use of overtime is having any material effect on the cost of the investigation to the user agencies?
  - *DCSA stated that overtime is not leading to increased costs at present.*

### **Defense Office of Hearings and Appeals (DOHA) Update**

- Peregrine Russell-Hunter, Director, delivered the update, noting that DOHA is the independent provider of a transparent and consistent process for not only DoD contractors but also the contractors for 32 other federal departments and agencies.
- DOHA remains timely on legal reviews of Statements of Reasons (SORs), which is important because that is the notice to the individual of what the concerns are with their eligibility (“before we make someone worry about losing their job, we make sure that we are right about it”). That is the first of a set of essential protections for industry contractors that includes a fair and independent hearing and the right to appeal an adverse decision.
- DOHA is leveraging technology to get hearings set and completed faster and is now conducting more than 85% of hearings virtually.

- DOHA is committed to transparency. If you call DOHA, you will get answers.

### **CUI Update**

- David Means, Program Analyst, ISOO, provided the update.
- ISOO highlighted the items that the government is required to add to contracts in which vendors may be expected to create, handle, or otherwise utilize CUI.
- ISOO described the chain of command pertaining to CUI and encouraged Industry personnel to reach out to their contracting officer and/or their agency's CUI Program Manager with CUI concerns before contacting ISOO.

### **Comments on CUI Update**

- A member of the public asked what actions ISOO is taking to ensure CUI is formally incorporated into any future update of EO 12829.
  - *ISOO's responsibility is to engage with Industry and across government to understand issues and raise recommendations to the NSC and the President, but ultimately, policy direction flows from the White House down.*

### **CMMC Update**

- Stacy Bostjanick, Chief Defense Industrial Base Cybersecurity, Deputy Chief Information Officer for Cybersecurity (DCIO(CS)), Office of the Chief Information Officer, delivered the update.
- 300-400 companies have been assessed for CMMC compliance to date. The total volume of companies to be assessed is around 220,000.
- DoD emphasized the need for companies to become cyber secure and meet the basic standards of NIST 800-171.
- The Defense Federal Acquisition Regulation (DFAR) clause 252.204-7021 is currently going through the rule making process.
- In December 2024, DoD issued 32 CFR Part 170.
- The 48 CFR rule will be subject to a period of public comment.

### **General Discussion, Remarks and Adjournment**

- Matthew Roche, NISP Mission Performance Division Chief, Industrial Security, DCSA, stated that there is an informational paper that is circulating that covers material change



to the SF-328, how those are defined, and what meets that standard. If anyone would like to view the paper, contact Isaiah Rivers or DCSA.

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

A handwritten signature in black ink, appearing to read "Michael D. Thomas". The signature is stylized, with the first name "Michael" written in a cursive-like script, followed by "D." and "Thomas" in a more formal, blocky style.

Michael Thomas  
Director, Information Security Oversight Office (ISOO)  
Chairman, National Industrial Security Program Policy Advisory Committee (NISPPAC)

Enclosure 1: Agenda  
Enclosure 2: Meeting Attendees  
Enclosure 3: New NISPPAC Bylaws  
Enclosure 4: Summary of Action Items  
Enclosure 5: Public Questions & Answers  
Enclosure 6: Meeting Slides

## **Enclosure 1: Agenda**

<b>Welcome</b>	10 mins
<b>Introductions</b>	5 mins
<b>Administrative Matters</b>	5 mins
<b>Vote on NISPPAC Bylaws</b>	5 mins
<b>Reports and Updates</b>	
• Industry Update	20 mins
• Department of Defense (DoD) Update (Executive Agent)	20 mins
• Defense Counterintelligence and Security Agency (DCSA) Update	20 mins
• Office of the Director of National Intelligence (ODNI) Update (Security Executive Agent)	10 mins
• Central Intelligence Agency (CIA) Update	5 mins
• Department of Homeland Security (DHS) Update	5 mins
• Department of Energy (DOE) Update	5 mins
• Nuclear Regulatory Commission (NRC) Update	5 mins
<b>Break</b>	10 mins
• Working Group (WG) Update	
○ DOE	5 mins
○ NRC	5 mins
○ DCSA NISP Cybersecurity Office (NCSO)	10 mins
○ DCSA Adjudication and Vetting Services (AVS)	10 mins
• Defense Office of Hearings and Appeals (DOHA) Update	5 mins
• Controlled Unclassified Information (CUI) Update	5 mins

- Cybersecurity Maturity Model Certification (CMMC) Update 15 mins

**General Discussion, Remarks and Adjournment** 5 mins

## Enclosure 2: Meeting Attendees

Adam Halk	Barbara Ruiz	Chris Heilig
Adam MacVean	Ben Parnelli	Chris Maclauchlan
Adam Mitchell	Benjamin Douglas	Christi Pattison
Adrian Shepherd	Benjamin Rogers	Christina Bracci
Alexa S. Emerson	Berette Smith	Christina Duke
Alexis Brown	Beverlee Kennedy	Christina Guatemala
Alexis VanDyke	B'Linda Thompson	Christina Jett
Alison K-V	Bonnae Vega	Christina King
Alison McGrath	Booker Bland	Christine Morris
Alison Norris	Bradley Tiffie	Christine Oppenhagen
Alissa Stone	Brandi M. Bell	Christopher Stolkey
Allison Fink	Brett Henderson	Chuck Spencer
Allyson J. Emerson	Brett Hill	Cindy Daniel
Allyson Renzella	Brett Rosenberg	Cindy Powell
Alyssa Heavner	Brian Murphy	Conrad Hertzog
Alyssa Heward	Brooke Fuemmeler	Constantine Dangas
Amanda Brien	Brooke Hall	Cooper Bell
Amanda Johnston	Caitlin Bonnett	Cory Dewyer
Amanda McGlone	Calvin Jetton	Crisaldo Padilla
Amanda Povsner	Candice Kagey	Crystal Husick
Amanda Upton	Candy Best	Crystal Michele
Amelia Baldree-Nichols	Carla Cobbs	Crystal Smith
Aminah Williams	Carlos Young	Crystal Smith
Amy Davis	Carmen Leisinger	Cynthia Hohweiler
Amy Lightcap	Carmen Zimmerman	Cynthia Silveira
Amy Terrell	Carol Garner	Dan Finucane
Anaia Janifer	Carole White	Dan Ly
Anastasia Obis	Carolina Klink	Daniel Agnew
Andrea Royal	Cary Iden- Parker Tide	Danielle McKenna
Andrew Roswal	Catherine Coburn	Daphne Cuffman
Andrianna Backhus	Catherine Kaohi	Darren Quarles
Andy Hernandez	Catherine Kaohi	David Cattler
Angelica Allen	Cathy Rickell	David Dayton
Anne Farmer	Chad Coffin	David Joe
Annette Simonson	Chad Noles	David Means
Anthony Finklea	Chad Plesakov	David Scott
Anthony Pinn	Chamagne Rodriguez	Dawn Hoffmann
Antoinette Thomas	Chantel Pettengill	Dawn Schulze
Arlene Talaro	Chantelle Dousay	Dean Miller
Ashley Bryan	Charles Phalen	Deanna Caputo
Ashley Mathias	Charles Tate	Debbie Sjodahl
AyCee Nash	Charlie Sowell	Debra Godbold
Barb Malloy	Charron Patterson	Diana F Thornton
Barbara Hanson	Chris Bujalski	Diana Payne

Diane Gibbs  
Diane Wallerson  
Dominic Ranc  
Don Edmunds  
Donna Avila  
Donna Ciccotosto  
Donna Huber  
Donna McLeod  
Donnie Lewis  
Doreen Villemaire  
Douglas Bletcher  
Douglas Oliver  
Dustin Glasoe  
Ed Otto  
Edith Mate  
Elicia Voorhies  
Elizabeth Sanchez  
Eloise Ziegler  
Emilio Matt  
Emily Heward  
Emily Pitek  
Emily Riley  
Emily Shanahan  
Eric Crytzer  
Eric Lally  
Erika Lasek  
Erin Young  
Eva Gonzales  
Evan Isaacs  
Fancheska Quinones  
Faye Mason  
Frances O'Rourke  
Frank Bradley  
Gabriel Garcia  
Gabriel Solis  
Gary Nolan  
Gene Griffe  
Geoffrey Dickey  
Geraldine Piccioni  
Geraldine Rogers  
Gina Chiocchio  
Gina Mills  
Ginger Lord  
Glenn Bensley  
Gloria A Sutton  
Glynn Davis

Grace Ziegler  
Grant Banks  
Grant Mayberry  
Greg Dubay  
Greg Pannoni  
Gregory Estevez  
Gregory Sadler  
Gus Greene  
Gwen Douglas  
Hanni Vitoritt  
Heather Erickson  
Heather Gardner  
Heather Harris Pagán  
Heather Hascall  
Heather Perez  
Heather Weaver  
Helencia Hines  
Howard High  
Iryna White  
Isaiah Rivers  
Jack Kearney  
Jacob Ziegler  
Jaime Gordon  
Jaime Waggoner  
James Burris  
James Favuzzi  
James Kester  
James Massaro  
James McAlary  
James Memole-Doodson  
James Pritchard  
James Ulery  
Jamie Atkinson  
Jamie Chapman  
Jane Gary  
Jane Dinkel  
Jane Sharma  
Janice Custard  
Jarvis Bell  
Jason Kobus  
Jason Smith  
Jason Steinour  
Jason Zieminski  
Jean Willett  
Jeff Grenier  
Jeff McOrmond

Jeffrey Spinnanger  
Jennie Hardy  
Jennifer Graham  
Jennifer May  
Jennifer Mosier  
Jennifer White  
Jessica Condon  
Jessica Flora  
Jessica Lee  
Jessica Q.  
Jessica VanDenBerg  
Jill Johnson  
Jim Donahue  
JoAnn Webber  
Joanna Sutphin  
Jocelyn Alexander  
Joe Schultz  
John Andrews  
John Motherway  
John.Cabe  
Johnathan Filiatrault  
Johnny Powell  
Jon Persinger  
Jonathan Fitz-Enz  
Joni Tucker  
Joseph Kraus  
Joshua Defibaugh  
Joyce Ramsey-Johnson  
Judith Fraser  
Juli MacDonald  
Julia Kearns  
Julia Ruffini  
Julie Clapp  
Julie Senatore  
Juliette Finch  
Justin J. Brocks  
Kacey Flanagan  
Kamilya Kamilova  
Kara Esposito  
Karen L. Kitts  
Kasey Funicello  
Kat Tran  
Katayoun Izadi  
Kate Dickerson  
Kathryn Jensen  
Kathy Andrews

Kathy Weakley  
Kay Hawkins  
Kayla Wilkinson  
Keith Minard  
Kellie OBrien  
Kelly Garvin  
Ken Hagood  
Kendall E. Adams  
Kenneth Hagood  
Keshia Washington  
Kevin Page  
Kia Gravely  
Kim David  
Kim Murphy  
Kimala Riche  
Kimberly Bemah  
Kimberly Gleason  
Kimberly Hunt  
Kimberly LaMont  
Kirsten Stutts  
Kristen Werkheiser  
Kristi Erb  
Kristin Smith  
Kristina Eddins  
Kristine Neilson  
Kyle Barton  
Kyle McKay  
Kyren J. Emerson  
Larry Clark  
Larry J. Rosales Jr.  
Larry Paxton  
LaToya Coleman  
Laura Aghdam  
Lauren Chase  
Lauren Jiggetts  
Laurie B.  
Laurie Christian  
Leandra Mosher  
Leonard Moss Jr.  
Lesley Gunn  
Leslie Aubert  
Leslie McCarthy  
Linda Bouthillette  
Linda Ginder  
Linda Jones  
Linda McCoy

Linda Propst  
Lindsey McNichol  
Lindsey McNichol  
Linwood Jongema  
Lisa Lynch  
Lisa Butz  
Lisa Freeman  
Lisa Measures  
Lisa Showell  
Lizliana Rubio  
Lorena Funicello  
Lori Ellison  
Lori Miller  
Lorisa Robles  
Lost Okies  
Lucas Bosch  
Makayla Brunk  
Makayla Marshall  
Manoj K  
Marcus Carpenter  
Maria Lancaster  
Maria Smith  
Marie Powell  
Mark Eckel  
Marlene Torres  
Mary Edington  
Maryellen Pryor  
Matthew Cawley  
Matthew Grinnell  
Matthew Kitzman  
Matthew Peoria  
Matthew Redding  
Matthew Roche  
Megan Schulze  
Mekdes Adissu  
Melinda Taylor  
Melissa Busch  
Melissa Butler  
Melissa Etters  
Melissa Poinelli  
Michael Driscoll  
Michael Hawthorne  
Michael Hulet  
Michael Lambuth  
Michael Marks  
Michael Petersen

Michael Thomas  
Michelle Einsmann  
Michelle Stallings  
Michelle Taylor  
Michelle Thompson  
Mike Faller  
Mike Sullivan  
Minh Le  
Mitch Lawrence  
Monica Marks  
Nathan Bujalski  
Nicholas Mirus  
Nicki Pona  
Nicolas Fichera  
Nicole Cooper  
Nicole Flynn  
Nicole Kastle  
Nicole Malbone  
Niel Hernandez  
Nikki Abrams  
Nina Gurman  
Nissa Dahle  
Norman Pashoian  
Olivia Johnson  
Pamela Hamilton  
Pamela Lawson  
Patrice Singletary  
Patricia Reynolds  
Patrick Harris  
Patrick McIntosh  
Patrick Sargent  
Patrick Webb  
Patton Bell  
Paula Green  
Paula Wright  
Paulicia Larkin  
Peregrine Russell-Hunter  
Perez, Carole  
Peter Mullin  
Quaintoinette "Von" Abney  
Quinnatt Jones  
Quinton Wilkes  
R. Scott III  
Rachel Ziegler  
Rae Yugas  
Randal LeBlanc

Raquel Franck  
Rebeca Pickering  
Rebecca Davis  
Rene Gutierrez  
Rene Haley  
Rich DeJausserand  
Rich Winsor  
Richard Leau  
Richard Ray  
Richard Wakeman  
Richard Whitney  
Rick Burgos  
Rigoberto Rodriguez  
Rob Deck  
Rob Manson  
Robert Brown  
Robert Escobedo  
Robert Gould  
Robert Oates  
Robert Vogt  
Robin Collo  
Rojohn Soriano  
Ronald Creech  
Ronald Young  
Russel Justice  
Rusty Jones  
Ryan Granger  
S. Dawn Hamilton  
Samantha Call  
Samantha Lichay  
Sami Riddle  
Sandra Daniel  
Sara Lindenmuth  
Sarah Stull  
Scarlett McKemy  
Scott Cronin  
Scott Glassic  
Scott Stewart  
Scott Stull  
Scott Sumner  
Sean Blackman  
SeKitha Nunn

Shala L. Romandelvalle  
Shannan Lunar  
Shannon Brown  
Shannon Farrell  
Shasta Kirkpatrick  
Shawn Yuthsakdidecho  
Shellie Schuler  
Sherrie Mason  
Sherry Nance  
Shirley Sims  
Spencer Manning  
Stacey D'Anthony  
Stacey Nagle  
Stacy Bostjanick  
Stacy Ortiz  
Stephanie Sneed  
Stephanie Thomas  
Steve Barbieri  
Steve Rosera  
Steven Blais  
Steven Brain  
Steven Chambers  
Steven McNeill  
Stewart D. Bell  
Susan Kubik  
Suzanne Eckerstrom  
Suzy Wendt  
Tamiko Pickering  
Tammi Chiappone  
Tammy Breediing  
Tammy Lepak  
Tammy Nolette  
Tara Wolf  
Ted Banks  
Teresa Hogan  
Terri McCoy  
Terri Powers  
Tessa Dutko  
Thang Lichay  
Thomas Cardella  
Thomas Hazlett  
Tiffany L. Lewis

Todd Flick  
Todd Soos  
Tomi Ajiboye  
Tony Pona  
Tonya Gray  
Tracey Henry  
Tracey Kumpel  
Tracy Cassidy  
Tracy Durkin  
Tracy Rixmann  
Treva Alexander  
Trina Everett  
Trina Everett  
Trish Brokenik  
Tristan Fielder  
Troy Arwine  
Twila Garrity  
Tyler Johnson  
Valerie Kerben  
Valerie McMichael  
Valerie Pylant  
Valerie Tarantino Setneska  
Vannessa Leach  
Vannessa Wilson Leach  
Vaughn Simon  
Vickie Sipes  
Wailohia Woolsey  
Wayne Lajoie  
Wendy Mills  
Wendy Mitchell  
Wendy Perez  
Wilda Fallen  
William Fournier  
William Linthicum  
William Tully  
Yvette Andablo  
Yvonne Jordan  
Zachary Ziegler  
Zahrah Madison  
Zak Beauregard  
Zoey Wright  
Zorica Ambrose

## **Enclosure 3: NISPPAC Bylaws**

### **Article 1. Purpose.**

The purpose of the NISPPAC, hereinafter referred to as the Committee, is to advise the Director, Information Security Oversight Office (ISOO), hereinafter referred to as the Chairperson, on all matters concerning the policies of the National Industrial Security Program (NISP), including recommended changes to those policies; and to serve as a forum to discuss policy issues in dispute.

### **Article 2. Authority.**

Executive Order 12829, "National Industrial Security Program," as amended, (the Order) establishes the Committee as an advisory committee acting through the Director, Information Security Oversight Office (ISOO), who serves as the Chairperson of the Committee, and who is responsible for implementing and monitoring the NISP, developing directives implementing the Order, reviewing agency implementing regulations, and overseeing agency and industry compliance. The framework for the Committee's membership, operations, and administration is set forth in the Order. The Committee is subject to the Federal Advisory Committee Act (FACA), the Freedom of Information Act (FOIA), and the Government in the Sunshine Act (GISA).

### **Article 3. Membership.**

**A. Primary Membership.** The Order conveys to the Chairperson the authority to appoint all members. There will be 16 representatives, including the Chairperson, from executive branch departments and agencies most affected by the NISP and eight non-government representatives of contractors, licenses, or grantees involved with classified contracts, licenses, or grants, for a total of 24 voting members. At least one industry member shall represent small business concerns, and at least one industry member shall represent the Department of Energy/Nuclear Regulatory Commission contractors or licensees. An industry member serves as a representative of industry, not as a representative of their employing company or corporation. All members must comply with the following guidelines:

(1) Any federal employees who are appointed to the Committee must file a confidential financial disclosure report on an annual basis, with the National Archives and Records Administration (NARA) Office of General Counsel (NGC) starting before the date of their first participation in a Committee meeting.



(2) If the initial or annual financial disclosure is not received by the NGC by the established deadline, then the representative will be unable to continue serving in that capacity until the financial disclosure is received.

(3) For purposes of federal ethics law, the non-federal members of the Committee have been determined to be "representatives" rather than "special government employees."

NARA will ensure the Committee's non-federal composition does not violate President Obama's June 18, 2010, Presidential Memorandum on "Lobbyists of Agency Boards and Commissions" 75 Fed. Reg. 35,955 (Directing "heads of executive departments and agencies not to make any new appointments or reappointments of federally registered lobbyists to advisory committees or other boards and commissions...")

**B. Nomination Process for Government Representatives.** The Chairperson will solicit and accept formal nominations for Committee membership from the agency head or the Senior Agency Official (SAO) for the NISP, however, a person may not nominate themselves. If the nomination from the SAO for the NISP or agency head is not received by the Chairperson on or before the date of their first participation in a Committee meeting, then the representative will not be able to vote during the Committee meeting and will be unable to continue serving as a Committee member until the appropriate nomination is received.

**C. Nomination Process for Non-government Representatives.** The Chairperson will solicit and accept formal nominations for Committee membership for non-government representatives through the Committee industry spokesperson designated in accordance with Article 3, paragraph E. They are responsible for ensuring the solicitation of nominations from the other non-government representatives on the Committee and from the governing boards of professional, trade and other organizations whose membership is substantially comprised of employees of business concerns involved with classified contracts, licenses, or grants. Although a non-government representative does not represent his or her employing company, the Chairperson will solicit the approval of the Chief Executive Officer or senior management official of that company to allow the nominated individual to serve on the Committee.

Each non-government Committee member and professional organization will be permitted to submit one nomination each to replace the two outgoing non-government Committee members whose terms end September 30 of that fiscal year (FY), or vacancies that occur during that FY but prior to September 30. Nominations from such professional, trade and other organizations must be endorsed by the board of the nominating organization. No such endorsement is necessary for nominations from the current Committee non-government members.

Nomination packages must include a resume, at minimum, and any other information that supports a nominee's qualifications for non-government Committee membership.

The industry spokesperson will select a former non-government Committee representative to convene a panel comprised of all the current non-government Committee representatives and the chairpersons of the professional organizations which have submitted a nomination to review all the submitted nomination packages.

Each non-government Committee member is allowed a total of two votes; one for each individual they determine will best represent industry to replace the two outgoing non-government Committee members, but they must ensure alignment with the criteria established in paragraph 12 of the Committee charter for non-government members.

While non-government Committee members represent all of industry and do not represent their respective company organizations, nominees who are employed by a company that already has current representation on the Committee will not be considered.

The industry spokesperson will ensure the nomination process is completed to allow sufficient time to transition the two incoming non-government Committee members by October 1 of the new FY.

At the conclusion of the vote, the industry spokesperson will provide the Chairperson with a copy of all submitted nomination packages and an endorsement of the two nominees to the Chairperson for consideration.

The Chairperson will request management approval from the companies employing the two endorsed nominees for their participation on the Committee for a four-year period. If company management cannot approve participation of a nominee, that individual will no longer be considered for Committee membership. The Chairperson will request that the panel endorse a replacement nominee from the pool of submitted nominations.

The Chairperson is not obligated to select a panel-endorsed nominee. Such a determination by the Chairperson should only be under exceptional circumstances, with rationale provided to the industry spokesperson. Should this occur, the panel will reconvene to identify a replacement nominee for consideration.

**D. Appointment.** The Chairperson shall initially appoint all Committee members. Members are required to attend Committee meetings. A member may select one or more alternates, who may, with advance written notification to the Chairperson, and with the approval of the Chairperson, when the primary member is unable to attend, serve in place of the primary

member at Committee meetings. Selected alternates shall have all the rights and authorities of the appointed primary member. If a member consistently misses meetings, the Chairperson may remove them as a member.

**E. Term of Membership.** The term of membership for Government representatives will conclude when they leave their current position, choose to no longer participate in the Committee, or are no longer a member by decision of the Chairperson. If their nomination letter states a term end date, a new letter is required to be provided prior to that term ending.

The term of membership for industry representatives is four years. The terms of industry representatives must be staggered so that the terms of two industry representatives are completed at the end of each FY. Industry representatives may not serve successive terms unless a representative served for a period of no longer than two years of the immediately preceding term. When a member is unable to serve their full term, or when, in the view of the Chairperson, a member has failed to meet their commitment to the Committee, a replacement will be selected in the same manner to complete the unexpired portion of that member's term. Each representative's term of membership will be conveyed by letter from the Chairperson.

**F. Industry Spokesperson.** The industry spokesperson serves as the focal point representative to the Committee on behalf of the industrial base to coordinate collective points of view from the eight non-government Committee members on national security policy regulations. The industry spokesperson is responsible for representing the Committee non-government members at each Committee meeting, recommending to the Chairperson the addition or deletion of Committee working groups (WGs), and assigning and recommending industry leads and subject matter experts for Committee WGs.

The industry spokesperson is selected from among the eight current non-government members and nominated to the Chairperson for consideration and approval. An annual vote is required to determine who will be the industry spokesperson. There is no term limit for this position. The spokesperson is expected to be flexible for attendance at impromptu government meetings where industry representation is required. The spokesperson engages with various facets of industry, to include governing boards of professional, trade and other organizations whose membership is substantially comprised of employees of business concerns involved with classified contracts, licenses, or grants.

**G. Security Clearance.** If it becomes necessary to hold a classified meeting, members and those in attendance must possess a current security clearance at or above the level of the meeting's classification.

Clearance certification shall be provided in advance of the meeting to the Chairperson by the employing agency or company. ISOO and NARA's Security Management Division will verify that members have been approved for access to classified national security information and ensure that classified information utilized in association with a Committee meeting is managed in accordance with national policy (i.e., E.O. 13526, "Classified National Security Information").

**H. Compensation.** Federal Government employees serving on the Committee are not eligible for any form of compensation. If appropriated funds are available, the Government may pay travel and per diem for industry members at a rate equivalent to that allowable to Federal Government employees. Industry members will submit travel vouchers to the Executive Secretary within 15 days after each meeting.

**I. Observers.** Any NISP participating organization (industry or Government) may send observers to attend meetings of the Committee. Such observers will have no voting authority and will be subject to the same restrictions on oral presentations as any member of the public. As determined by the Chairperson, observers may be permitted to attend closed meetings. Industry observers will not be eligible for travel or per diem compensation.

#### **Article 4. Meetings.**

**A. General.** The Committee will meet at least twice each calendar year as called by the Chairperson. As the situation permits, the Executive Secretary will assess the membership in advance of the scheduling of meetings to facilitate attendance by the largest number of members. The Chairperson will also call a meeting when requested by a majority of the Government members or alternates and a majority of the eight industry members. The Chairperson will set the time and place for meetings and will publish a notice in the Federal Register at least 15 calendar days prior to each meeting.

**B. Quorum.** Committee meetings will be held only when a quorum is present. In this instance, a quorum requires the presence of at least a majority of the current members of the Board and shall not be fewer than three members of the government members and three of the industry members.

**C. Open Meetings.** Unless otherwise determined in advance, all meetings of the Committee will be open to the public. Once an open meeting has begun, it shall not be closed for any reason. All matters brought before or presented to the Committee during the conduct of an open meeting, including the minutes of the proceedings of an open meeting, shall be available to the public for review or copying.

If, during an open meeting, matters inappropriate for public disclosure arise during discussions, the Chairperson will order such discussion to cease, and shall schedule such discussions for a closed session.

**D. Closed Meetings.** Meetings of the Committee will be closed only in limited circumstances and in accordance with applicable law. When the Chairperson has decided in advance that discussions during a Committee meeting will involve matters about which public disclosure would be harmful to the interests of the Government, industry, or others, an advance notice of a closed meeting, citing the applicable exemptions of GISA, will be published in the Federal Register. The notice may announce the full or partial closing of a meeting. Notices of closed meetings will be published in the Federal Register at least 15 calendar days in advance.

**E. Agenda.** The Chairperson will approve the agenda for all meetings, and the final agenda will be provided to the members prior to each meeting. Suggested items for the agenda may be submitted to the Chairperson by any regular or alternate member of the Committee. Items may also be suggested by non-members, including members of the public. To the extent possible, all written recommendations for the NISP or National Industrial Security Program Operating Manual policy changes, whether they are placed on the agenda, will be provided to the Committee membership prior to the start of any scheduled meeting. The Chairperson will advise the party making the recommendation what action was taken or is pending.

**F. Conduct of Meetings.** Meetings will be called to order by the Chairperson. The Designated Federal Officer (DFO) will take roll call and reference the certified minutes of the previous meeting. The Chairperson will open the meeting. The DFO will provide announcements, ask for reports from subgroups or individual members (as previously arranged), open discussion of unfinished business, introduce new business, and invite membership comments on that business. Public comment and questions may be provided verbally or through written communication at any time during the meeting. Upon completion of the Committee's business, as agreed upon by the members present, the meeting will be adjourned by the Chairperson.

**G. Meeting Minutes.** The Committee's DFO shall prepare minutes of each meeting, which will be certified by the Chairperson within 90 calendar days. The agenda, minutes, attendee list, and presentations will be consolidated into a single "NISPPAC Meeting Report", posted on the ISOO website at <https://www.archives.gov/isoo/oversight-groups/nisppac/committee.html>, and will be accessible to the public. Copies of the meeting report will also be distributed to all Committee members and speakers once finalized. The minutes will include the time, date, and place of the Committee meeting, a list of the persons who were present at the meeting, including the names of committee members and staff, agency employees, and members of the public who presented oral or written statements, an accurate description of the each matter discussed and the

resolution, if any, made by the Committee regarding such matters, copies of each report received, issued or approved by the Committee at the meeting.

**H. Public Comment.** Members of the public may attend any meeting, or a portion(s) of a meeting that is not closed to the public, and may, at the determination of the Chairperson, offer public comment during a meeting. Also, members of the public may submit written statements to the Committee at any time.

**I. Sub-committee Meetings.** The Chairperson may establish a sub-committee(s), to include sub-groups or WGs. The Industry lead as determined by the Industry Spokesperson for each working group is responsible for approving industry attendees that are not currently Committee members. The DFO will be responsible for approving government attendees that are not currently Committee members. Each sub-committee/WG will brief the members of the Committee on its work, and any recommendations of a sub-committee/WG shall be presented to the Committee for deliberation.

## **Article 5. Voting.**

When a decision or recommendation of the Committee is required, it will be annotated on the agenda for awareness. The Chairperson will then request a motion for a vote during the public meeting. Any member or approved alternate of the Committee, including the Chairperson, may make a motion for a vote. No second motion after a proper motion shall be required to bring any issue to a vote.

**A. Voting Eligibility.** Only the Chairperson and the appointed members, or their designated alternates, may vote on an issue before the Committee.

**B. Voting Procedures.** Votes shall ordinarily be taken verbally, in writing, or tabulated by a show of hands. Results of votes will be annotated in the meeting minutes.

**C. Reporting of Votes.** The Chairperson will report to the President, Executive Agent of the NISP, or other Government officials the results of Committee voting that pertain to the responsibilities of that official. In reporting or using the results of Committee voting, the following terms shall apply:

(1) Unanimous Decision. Results when every voting member, except abstentions, are in favor of, or opposed to, a particular motion;

(2) Government and Industry Consensus. Results when two-thirds of those voting, including two-thirds of all Government members and two-thirds of all industry members, are in favor of, or are opposed to, a particular motion;

(3) General Consensus. Results when two-thirds of the total vote cast are in favor of, or are opposed to, a particular motion;

(4) Government and Industry Majority. Results when the majority of the votes cast, including a majority of all Government members and a majority of all industry members, are in favor of or are opposed to a particular motion;

(5) General Majority. Results when a majority of the total votes cast are in favor of or are opposed to a particular motion.

#### **Article 6. Committee Officers and Responsibilities.**

**A. Chairperson.** As established by the Order, the Committee Chairperson is the Director, ISOO. The Chairperson will: (1) call meetings of the full Committee; (2) set the meeting agenda; (3) determine a quorum; (4) open, preside over and adjourn meetings; and (5) certify meeting minutes.

**B. Designated Federal Officer.** The FACA requires each advisory committee to have a DFO and an alternate, one of whom must be present for all meetings. The Industrial Security Program Manager, ISOO, is the DFO for the Committee. The alternate DFO is one of ISOO's Committee staff. Any meeting held without the DFO or alternate present will be considered as a sub-committee/WG meeting.

**C. Executive Secretary.** The Executive Secretary shall be a member of the staff of the ISOO and shall be responsible for: (1) notifying members of the time and place for each meeting; (2) recording the proceedings of all meetings, including subgroups or working group activities that are presented to the full Committee; (3) maintaining the roll; (4) preparing the minutes of all meetings of the full Committee, including subgroups and working group activities that are presented to the full Committee; (5) attending to official correspondence; (6) maintaining official Committee records and filing all papers and submissions to the Committee, including those items generated by subgroups and working groups; (7) acting as Committee Treasurer to collect, validate and pay all vouchers for preapproved expenditures presented to the Committee; (8) preparing a yearly financial report; and (9) preparing and filing the annual Committee report as required by the FACA.

**D. Committee Staff.** The staff of the ISOO shall serve as the Committee staff on an as needed basis and shall provide all services normally performed by such staff, including assistance in the fulfilling of the functions of the Executive Secretary.

#### **Article 7. Documents.**

Documents presented to the Committee by any method at any time, including those distributed during a meeting, are part of the official Committee files, and become agency records within the meaning of the FOIA, and are subject to the provisions of that Act. Documents originating with agencies of the Federal Government shall remain under the primary control of such agencies and will be on loan to the Committee. Any FOIA request for access to documents originating with any agency shall be referred to that agency. Documents originating with industry that have been submitted to the Committee during its official business shall also be subject to request for access under FOIA. Proprietary information that may be contained within such documents should be clearly identified at the time of submission.

#### **Article 8. Committee Expenses and Cost Accounting.**

Committee expenses, including travel and per diem of non-Government members, will be borne by ISOO if appropriated funds are available for these expenditures. Cost accounting will be performed by the Committee's Executive Secretary. Expenditures by the Committee or any subgroup or working group must be approved in advance by the Chairperson or the Executive Secretary.

#### **Article 9. Amendment of Charter and Bylaws.**

Amendments to the Charter and Bylaws of the Committee must conform to the requirements of the FACA and the Order and be agreed to by two-thirds of the Government members or alternates and two-thirds of the eight industry members or alternates. Confirmed receipt of notification to all Committee members must be completed before any vote is taken to amend either the Charter or Bylaws.



## **Enclosure 4: Summary of Action Items**

- Industry requested that ISOO convene a meeting of the CSAs to discuss CUI.
- Industry requested a meeting with CSAs to discuss communication options so they are not surprised by future announcements. NRC and ODNI are the only two CSAs that need to respond, as the other CSAs responded during the public meeting.
- Industry requested a meeting to discuss reciprocity of training with CSAs and CSOs. Industry will need to provide specifics of when reciprocity is not taking place.
- Industry asked OUSDI&S to work with the military departments to expand the SCI Indoctrination authority for Industry, and work with them for a better process moving forward.
- Industry, requested that government inform Industry of any budgetary or personnel changes that will impact Authorizations to Operate (ATOs).
- Industry asked DCSA to provide a status update on the facility clearance orientation handbook.
- Industry requested that ISOO coordinate with the CSAs to provide guidance to Industry as soon as possible on all EOs with suspected NISP implications.
- Industry requested cooperation from the government in devising sanitization procedures for solid state drives involved in spills.
- Industry requested that DCSA provide a status update on the facility clearance orientation handbook.
- ODNI agreed to organize discussion within the IC on reciprocity of training.
- Industry requested OUSDI&S establish a vehicle for Industry to provide NBIS requirements and feedback and would like an initial meeting on this topic within 30 days.
- Industry requested to be a part of the policy making process regarding the covered insider threat policy with ODNI.
- Industry requested guidance from the services on expected timelines for SCIF and SAPF compliance.
- Industry asked for a meeting with the CSO of DHS.

## Enclosure 5: Public Questions & Answers

**\*Any questions not answered by publication will turn into Action Items for the next meeting for the appropriate response.\***

**Question:** Russell Justice asked: In regards to the CUI and CMMC discussions in today's NISPPAC meeting, I am seeking clarification on CMMC and in scope cloud service providers. For example, many companies in Industry utilize SaaS solutions for security management. These include solutions like SIMs, Tru-Vetting, Security Control, Sign-In Solutions, etc. These programs allow for upload of DD-254s, which are becoming more and more often CUI. Looking through the myriad of guidance on CMMC, it appears that FEDRAMP Moderate Equivalent is still acceptable and is on the contractor utilizing the service to assess required documents and ultimately take on the risk. Additionally, if they do not deal directly with the government, are they able to receive FEDRAMP Moderate certification? Who would be their sponsor? Most are applications that sit within an approved CSP such as AWS GovCloud. If I am not making sense, it only goes to show that the guidance for CMMC, 800-171, etc. are confusing, often contradictory, and not adequately distributed to Industry Partners. Beyond the security software solutions, you have the ERP solutions like Unanet...how far down the private industry chain does FEDRAMP or FEDRAMP equivalent reach? How can we continue to modernize and manage our contracts?

**Answer:** Not provided by responsible point of contact.

**Question:** Treva Alexander asked: What are the projected national security and economic implications of continuing to exclude CUI from the NISP framework, especially given that a lack of uniform handling procedures has already been shown to create confusion, compliance risk, and operational inefficiencies for contractors working across multiple agencies?

**Answer:** When it comes to managing sensitive information that the federal government possesses or handles, we agree that it is important when thinking of information management in this context to consider the broad spectrum of information ranging from Classified National Security Information to CUI to other unclassified information that the government handles. ISOO recognizes the need for a standardized approach to CUI, and that conversations regarding the NISP have understandably included discussion of CUI. Efforts such as CMMC and the proposed CUI Federal Acquisition Regulation (FAR) clause rules aim to help establish more uniform requirements for protecting CUI across federal agencies and Industry. As long as a single, overarching framework is not universally implemented, the risks of inconsistent CUI handling will continue to pose a threat to national security and economic competitiveness. Regarding incorporation of CUI into the NISP executive order, which dates from 1993 and well prior to the establishment of the CUI program, ISOO has advocated for the modernization of the NISP EO to the NSC, and the appropriate consideration of CUI within that framework would likely be part of those discussions.

**Question:** Nik A asked: 32 CFR Policy Question: E-Verify offers an accepted electronic method to validate citizenship. Can DoD/DCSA speak on any consideration to update the 32

CFR part 117.10 (C) NISPOM rule to validate original or certified copies of proof of citizenship to include language that supports a similar (if not the same) electronic method?

**Answer:** Not provided by responsible point of contact.

**Question:** Diana F. Thornton asked: When will the updated SF- 328 be available/distributed?

**Answer:** The form is available now. There has been a delay getting it posted to the GSA forms web site. It is available on the DCSA web site at <https://www.dcsa.mil/Portals/91/Documents/CTP/tools/SF328-18b.pdf>.

**Question:** Jennie Hardy asked: May we address the plan to address Industry's concerns with the hesitance of IC adopting initiatives to modernize systems and eventually adopt the PVQ aligning with the updated investigative standards. In speaking with individual agency PERSEC leads, there seems to be no foreseeable intent to modernize. This will continue to be problematic. (despite those agencies being under the same TW mandate).

**Answer:** Not provided by responsible point of contact.

**Question:** Russel Justice asked: If the security-in-depth (SID) is standardized due to reciprocity issues, doesn't that mean the new standard will just end up being the most strict requirements to satisfy all agencies?

**Answer:** No, it does not mean it will be the strictest standard to satisfy all agencies. The intent is to list a broad criterion that must be met in order to qualify as security-in-depth. It will not be a comprehensive list of what can be used to achieve SID.

**Question:** Mitch Lawrence asked: Will the 2024 ICD-124 be revised (details moved to the ICS)? As lengthy (18 pages?) ICD, it does not fit the ICD model.

**Answer:** The ICD is currently under review. The previous office serving as the accountable official (IC Human Capital) has been dissolved. The revision process to name a new accountable official in the ICD could potentially be part of a greater revision, but we do not have any information that this is being considered.

**Question:** Russel Justice asked: Did anyone catch if she said they are going to remove the US Persons and move to US Citizens? Does that mean for the entire process of construction?

**Answer:** The revision of the ICS and related discussions are still ongoing. Once the community has reached a consensus, we will report updates back to industry via the ISOO.

**Question:** Marlene Tores asked: Do we know how many companies are compliant with CMMC?

**Answer:** Not provided by responsible point of contact.

**Question:** Russel Justice asked: The number one question I get from people in my company is geared around in-scope systems. Programs that industry use like Unanet or SIMS that house CUI. Are they required to be FEDRAMP Moderate approved or can they show equivalency? If they don't have direct government customers, who sponsors them for FEDRAMP?

**Answer:** Not provided by responsible point of contact.

**Question:** Marlene Tores asked: Can you explain what FCI is in regards to CMMC?

**Answer:** Not provided by responsible point of contact.

**Question:** During the Physical Working Group, the Air Force was going to find out if they have timeline expectations on transfer of cognizance determinations. Did that happen?

**Answer:** Yes. The Air Force has coordinated internally and can share that transfers of cognizance (TOC) require Defense Intelligence Agency's (DIA) involvement and therefore are dependent on their resourcing and availability. There are also many factors that go into the timeline for a TOC if you have a non-DoD facility (i.e., CIA, Federal Bureau of Investigations (FBI), etc.). If a non-DoD facility already meets ICD 705 standards, it is reasonable to think it should not take more than 45-60 days for the TOC action to be processed once received by DIA. The key is ensuring the Special Security Officer (SSO) has all appropriate paperwork to provide when requesting the TOC. If they do not have all the required paperwork or there are issues with the facility then it can take additional time. Bottom line – It depends on several factors, but in a perfect scenario it reasonably should not take more than 45-60 days for the TOC action once it's with DIA. However, we recognize that DIA is under resourced, and their timelines have therefore been impacted.

Enclosure 6: Meeting Slides

# NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE

## PUBLIC MEETING



MAY 28, 2025

# PUBLIC WIFI



# A1 Guest

Click “Sign in”, and then click “Accept”



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION

# AGENDA



- Welcome
- Introductions
- Administrative Matters
- Bylaws Vote
- Reports and Updates
  - Industry
  - Department of Defense (DoD)
    - Defense Counterintelligence and Security Agency (DCSA)
    - Office of the Director of National Intelligence (ODNI)
    - Central Intelligence Agency (CIA)
  - Department of Homeland Security (DHS)
  - Department of Energy (DOE)
    - Nuclear Regulatory Commission (NRC)
- Break



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION



# AGENDA



- Working Group Updates
  - DOE
  - NRC
  - DCSA NISP Cybersecurity Office (NCSO)
  - DCSA Adjudication and Vetting Services (AVS)
- Topic Briefings
  - Defense Office of Hearings and Appeals (DOHA)
  - Controlled Unclassified Information (CUI)
  - Cybersecurity Maturity Model Certification (CMMC)
- General Discussion
- Closing Remarks
- Adjournment



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION



# OPENING REMARKS



## ISOO : Michael Thomas



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION

# OPENING REMARKS



ISOO :  
Jennifer May



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION

# REPORTS & UPDATES



## INDUSTRY : Ike Rivers



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION



# National Industrial Security Program Policy Advisory Committee (NISPPAC)

NISPPAC Industry Updates

May 2025



***THANK YOU  
Greg & Dave!***





# Industry's NISPPAC Current Members



## Welcome Chris!



Isaiah "Ike"  
Rivers  
Institute for  
Defense  
Analyses  
(IDA)  
2022 - 2026



Greg Sadler  
General  
Dynamics  
Information  
Technology  
2021 - 2025



Dave Tender  
ASRC  
Federal  
2021 - 2025



Jane Dinkel  
Lockheed  
Martin  
2022 - 2026



Kathy  
Andrews  
Northrop  
Grumman  
2023 - 2027



Chris Stolkey  
BAE Systems  
2024 - 2027



LaToya  
Coleman  
ManTech  
Int. Corp  
2024 - 2028



Charlie  
Sowell  
SE&M  
Solutions  
2024 - 2028



Lisa Reidy  
General  
Dynamics  
Information  
Technology

Industry NISPPAC  
Coordinator

Industry NISPPAC Members Uniting Industry



## WELCOME Christy

<b>Memorandum of Understanding (MOU) Industry Association Security Representatives</b>	
Heather Sims	Aerospace Industries Association (AIA)
	ASIS Defense and Intelligence Council (ASIS D&IC)
Robert Sanborn	Contractor Special Security Working Group (CSSWG)
Jason Hawk	Federally Funded Research and Development Centers/University Affiliated Research Centers (FFRDC/UARC)
Mary Edington	Intelligence and National Security Alliance (INSA)
Leonard Moss	Industrial Security Working Group (ISWG)
Darcy Fisher	National Classification Management Society (NCMS)
James Kennedy	National Defense Industrial Association (NDIA)
Christy Wilder	Professional Services Council (PSC)
Rosie Borrero-Jones	Community Association for Information Systems Security Working Group (CAISSWG)

# Industry Topics



## ALL CSA/CSO

- CUI – With so much confusion within Industry concerning CUI, will there be a sit down between all the agencies to finally discuss what each agency is going to do when it comes to CUI?
- Communication Channels – What communications vehicles/channels do you have with Industry to ensure that Industry is informed on real time and much needed information?
- Reciprocity of Training

## DoD

- CUI
- SCI Indoctrination Authority for Industry
- Solid State Drive
- NBIS – How is DoD working with DCSA regarding the NBIS issue. Also when is DoD or DCSA going to reach out to Industry and ask about requirements.



# Industry Topics



## DCSA

- Investigation Timelines Update
- PVQ Update – Status of the pilot with the two agencies. Is industry projected to also have pilot before rollout.
- NBIS Update – Will Industry get an opportunity to provide requirements.
- ATO Timeline Update – Also does industry anticipate delays if DCSA is effected by possible loss of staff
- FCL Timelines associated with each stage of the process – what is the recourse of not meeting the timelines
  - ❑ Update on FCL Orientation Handbook
- Staff Training Update regarding limiting inconstancies across the DCSA

## ODNI

- Covered Insider Threat Information Sharing Policy Update
- Overhead Billets Policy Update
- TORIS Update

# Physical Security Working Group Updates



## Updates since 22 January ISOO Meeting:

- Multiple ODNI/NCSC working group meetings (DCWG, ICISRM)
- Industry reinstated to attend PTSWG
- Strong collaboration with IC
- Monthly Industry NISPPAC Working Group meetings
- Companies developing POAMs

# Key Issues/Concerns/Ask

- Align all dates for compliance across Government
  - Clear guidance needed from Services re: SAPF
- Risk based approach to modifications to current facilities
- Response to POAMs submitted to date
- Continued concern regarding reciprocity across Government
- Innovative alternatives to achieve Tempest protection
  - Self testing by Industry (using certified CTTAs)





THANK YOU

# REPORTS & UPDATES



DOD :  
Jeff Spinnanger



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION

# DoD Updates



## ➤ Policy Updates

- 32 CFR 117
- DoDI 5220.32
- DoDM 5220.32 (Vol's 1 and 2)

## ➤ Focus Areas

- Systems and Data Interoperability
- Cybersecurity

## ➤ Continuing Priorities

- Information Security Reforms
- Acquisition Security Implementation

*“Security, cybersecurity, and protection of critical technologies at all phases of acquisition are the foundation for uncompromised delivery and sustainment of warfighting capability.” – DoDD 5000.01*

# REPORTS & UPDATES



DCSA :  
David Cattler



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION



# REPORTS & UPDATES



ODNI :  
Lisa Perez



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION





Office of the Director of National Intelligence

National Counterintelligence and Security Center

# ODNI Updates

Lisa Perez, Chief, Policy and Collaboration  
Tessa Dutko, Technical Security and Policy Officer





Office of the Director of National Intelligence

National Counterintelligence and Security Center

## Congressionally Directed Actions (CDAs) Overview

- 60 CDAs currently assigned to SSD
- 7 Industry-related CDAs, some of which are recurring
- Typically some of the heavier lift CDAs, require multiple data calls, external studies, and creation of new policies
- SSD is currently working 4 Industry CDAs, remaining 3 are contingent on other CDAs being completed first





## Office of the Director of National Intelligence

National Counterintelligence and Security Center

### Industry CDA Progress

1. **Policy on Submittal for Access to Classified Information for Key Management and Oversight Positions (IAA 2023 Section 6605)**
  - Fully drafted; in review with Office of General Counsel
2. **Requirement to Authorize Additional Security Clearances for Certain Contractors-Study (IAA 2024 Section 7505(b))**
  - Data calls complete; MITRE is starting to draft
  - Includes another CDA section that is contingent on the completion of the study
3. **Policy on Sharing of Covered Insider Threat Information Pertaining to Contractor Employees (IAA 2022 Section 806)**
  - Reworked to better address Congress' requirement; in NSCS's internal coordination
  - Includes another CDA section that is contingent on the completion of the policy
4. **Reports on Expansion of Security Clearances for Certain Contractors (IAA 2023 Section 6715(c))**
  - Awaiting results from one more data call before finishing the draft for FY 23 and FY 24
  - Includes another CDA section that is contingent on the completion of the above reports



Office of the Director of National Intelligence

National Counterintelligence and Security Center

# ***Security Executive Agent Directive 4 Review***



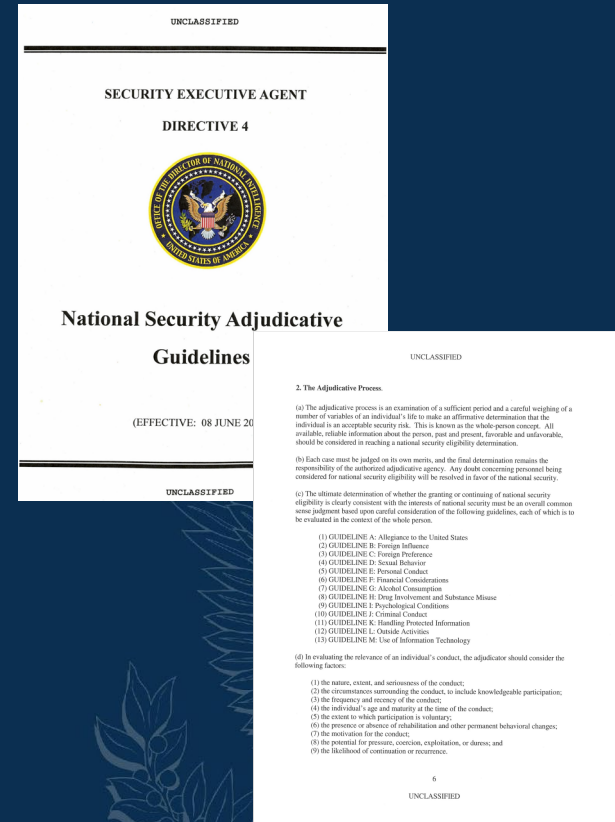


## Office of the Director of National Intelligence

National Counterintelligence and Security Center

The Security Executive Agent Directive (SEAD) 4 National Security Adjudicative Guidelines are a comprehensive framework used to evaluate an individual's eligibility for access to classified information or to hold a sensitive position.

- ❑ 13 individual guidelines
- ❑ Mandates the use of the "whole person" concept
- ❑ "Eligibility for access....shall only be granted when....clearly consistent with the interests of the United States; any doubt shall be resolved in favor of national security..."



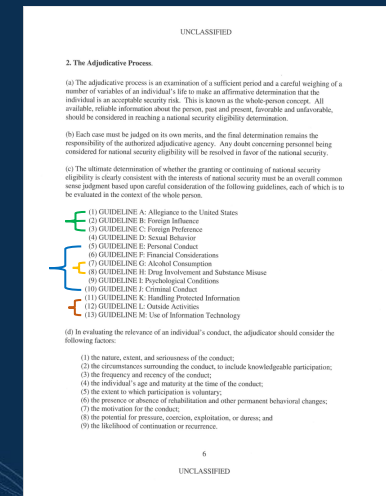


# Office of the Director of National Intelligence

National Counterintelligence and Security Center

## Adjudicative Guidelines Review: Approach— Ensure alignment to TW 2.0

**Refresh Review:** Comprehensive, deliberate, analytical, review of the guidelines to ensure they are still effective, efficient, and promote uniformity in adjudications. We will leverage research, previous case damage assessments, and look at all of the adjudicative concerns.







## Office of the Director of National Intelligence

National Counterintelligence and Security Center

### **Adjudicative Guidelines Review Notional Timeline**

#### **Refresh Review**

- Initial scoping meeting completed
- Research and literature review ongoing
- Small interagency working groups Q2-3 FY25
- Formal interagency working groups Q3-4 FY25
- Draft Product early FY26
- Publish ~Q4 FY26-Q1 FY27





Office of the Director of National Intelligence

National Counterintelligence and Security Center

# ***Trusted Workforce 2.0***







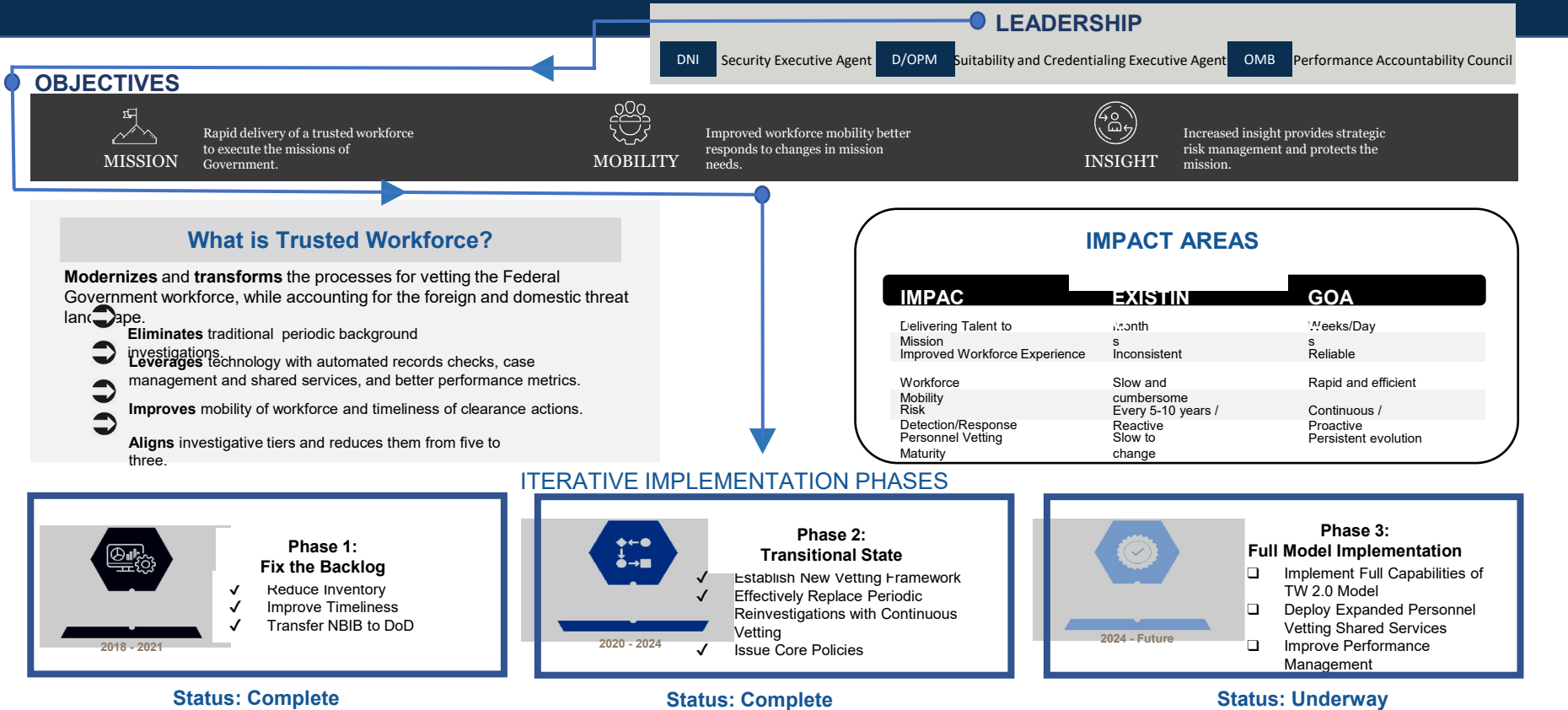
# Office of the Director of National Intelligence

National Counterintelligence and Security Center

## TRUSTED WORKFORCE 2.0

Mission • Mobility • Insight

### Overview





Office of the Director of National Intelligence

National Counterintelligence and Security Center

# ICD 705 Upgrades and Compliance

- D/NCSC Memorandum (NCSC 2024-00157): *Required Plans of Action for Complying with ICD 705*
  - Notes the increase in physical and technical threat to SCIFs
  - Identification of SCIFs that do not meet current ICD 705 standards, to include TEMPEST countermeasure requirements
  - Prioritize SCIFs for upgrade
  - Complete POAMs by December 2025
  - Upgrades complete by December 2028





Office of the Director of National Intelligence

National Counterintelligence and Security Center

# ICD 705 Updates

- IC Standard (ICS) 705-01, *Physical and Technical Security Standards for SCIFs*
- ICS 705-03, *Acoustic Standards for SCIFs*
- ICS 705-04, *Foreign Partner Physical Access to U.S. SCIFs*
- ICS 705-05, *Physical and Technical Security Standards for Data Center SCIFs*





Office of the Director of National Intelligence

National Counterintelligence and Security Center

# Policy Updates Impacting ICD 705

- ICS 702-01, *Technical Security and Signals Countermeasures (TSSC) for SCIFs*
- ICS 124-01, *Electronic Medical Device Review Process and Reporting Requirements*



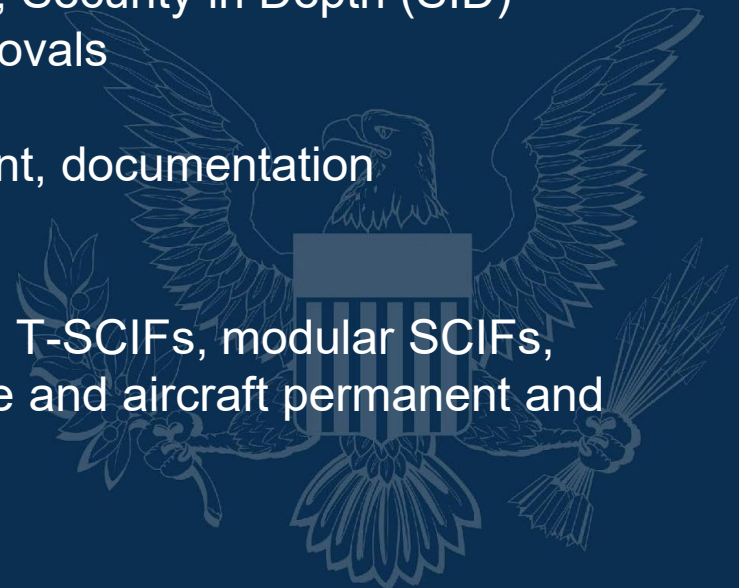


Office of the Director of National Intelligence

National Counterintelligence and Security Center

# ICD 705 Technical Specifications

- All 14 chapters currently being revised/coordinated with the IC
- Targeted date of completion, end of calendar year 2025
- Chapter 2 – Updated risk assessment process, Security in Depth (SID) requirements, Compartmented Area (CA) approvals
- Chapter 3 – Updated construction, management, documentation requirements
- Chapter 6 – Adding section on executive travel T-SCIFs, modular SCIFs, and separate chapters on shipboard/submarine and aircraft permanent and T-SCIFs





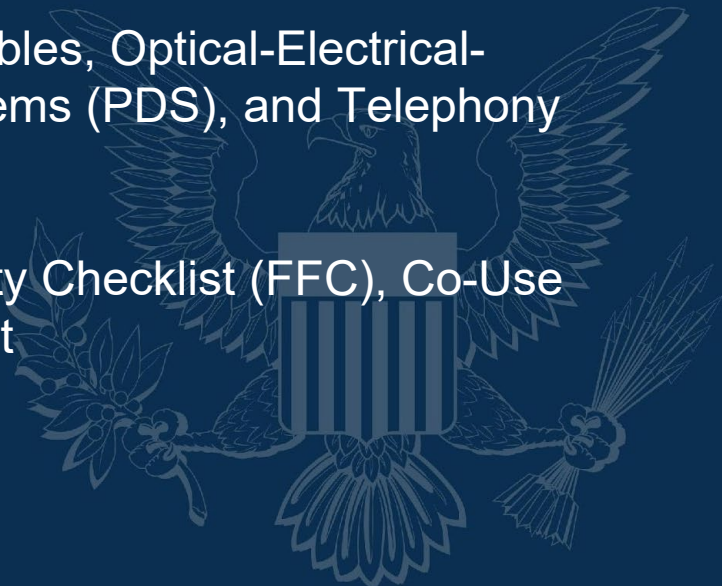


Office of the Director of National Intelligence

National Counterintelligence and Security Center

# ICD 705 Technical Specifications

- Chapter 9 – Updating acoustic testing requirements to align with ICS 705-03
- Chapter 10 – Updating guidance on Personal Electronic Devices (PEDs)
- Chapter 11 – Adding guidance on fiber optic cables, Optical-Electrical-Optical conversion, Protected Distribution Systems (PDS), and Telephony Equipment
- Chapter 14 – TEMPEST Checklist, Fixed Facility Checklist (FFC), Co-Use Agreement, CA Checklist, and T-SCIF Checklist





Office of the Director of National Intelligence

National Counterintelligence and Security Center

# NCSC Engagement with Industry

- IC Industry Security Representatives Meeting (ICISM)
- Physical and Technical Security Expert Working Group (PTSEWG)
- Data Center Working Group (DCWG)



# REPORTS & UPDATES



CIA :  
Don



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION



# REPORTS & UPDATES



DHS :  
Rich Dejausserand



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION

# REPORTS & UPDATES



DOE :  
Jaime Gordon



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION



# DOE Updates

**Q:** How often does DOE perform a business assessment?

**A:** Analysis of companies in process for a facility clearance and those reporting a changed condition or material change to previously submitted information in the National Industrial Security Program is completed within eFOCI, our system of record. DOE completes formal business assessments, or a variation thereof, on a case-by-case basis in select offices based on resources.

**Q:** What communications vehicles/channels do you have with Industry to ensure that Industry is informed on real time and much needed information?

**A:** Policy Panel meetings and various working groups throughout the year

- PPMPP – Program Planning and Management Policy Panel
- STWG – Systems Testing Working Group
- PTWG – Performance Testing Working Group
- SASIG – Security Awareness Shared Interest Group
- EFWG - DOE Entity Eligibility Determination (EED)/Foreign Ownership, Control, or Influence (FOCI) Working Group
- EFCOG – Energy Facility Contractors Group

# REPORTS & UPDATES



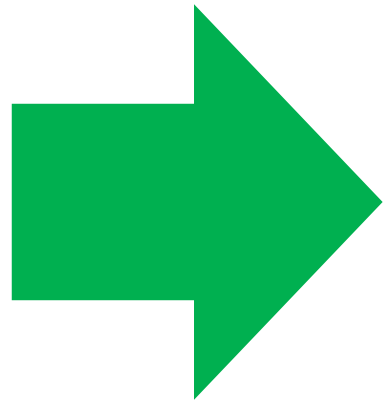
NRC :  
Chris Heilig



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION

# BREAK



**RETURN IN :  
15 MINUTES**



**NISPPAC  
PUBLIC  
MEETING**

**MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION**

# WORKING GROUPS



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION



# WORKING GROUPS



DOE :  
Jaime Gordon



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION



---

# Workload & Timeliness Performance Metrics

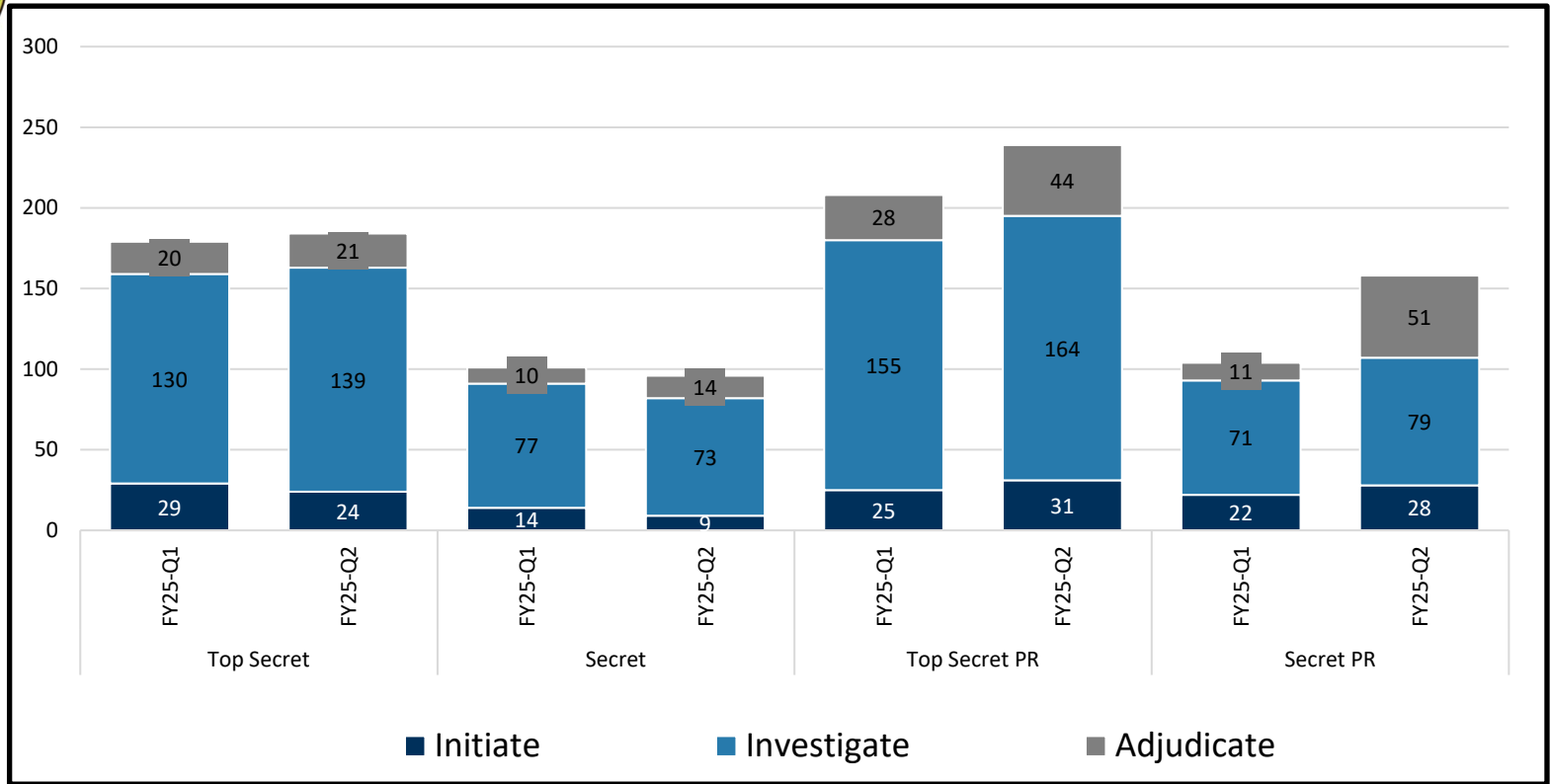
---

Department of Energy





# Average Days for Fastest 90% of Reported Clearance Decisions Made – Contractor Investigations



Total Adjudications Reported					
	Top Secret	Secret	Top Secret PR	Secret PR	Totals
FY25-Q1	1,874	567	322	175	2,938
FY25-Q2	1,860	587	307	102	2,856



# Pending Adjudications by Clearance Level

Pending Contractor Adjudications	
Top Secret	631
Secret	239
Top Secret PR	213
Secret PR	69
TOTAL	1,152



# DOE Points of Contact

## **Jaime Gordon**

Program Planning and Management, Office of Security Policy

Phone Number: (240) 687-3439

Email Address: [jaime.gordon@hq.doe.gov](mailto:jaime.gordon@hq.doe.gov)

## **Monica Marks**

Acting Director, Office of Departmental Vetting Policy and Outreach

Phone Number: (202) 586-4558

Email Address: [monica.marks@hq.doe.gov](mailto:monica.marks@hq.doe.gov)

## **Theodore Banks**

Due Diligence Program Manager, Office of Headquarters Industrial Security Operations

Phone Number: (202) 287-1758

Email Address: [theodore.banks@hq.doe.gov](mailto:theodore.banks@hq.doe.gov)

# WORKING GROUPS



NRC :  
Chris Heilig



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION

# WORKLOAD & TIMELINESS PERFORMANCE METRICS

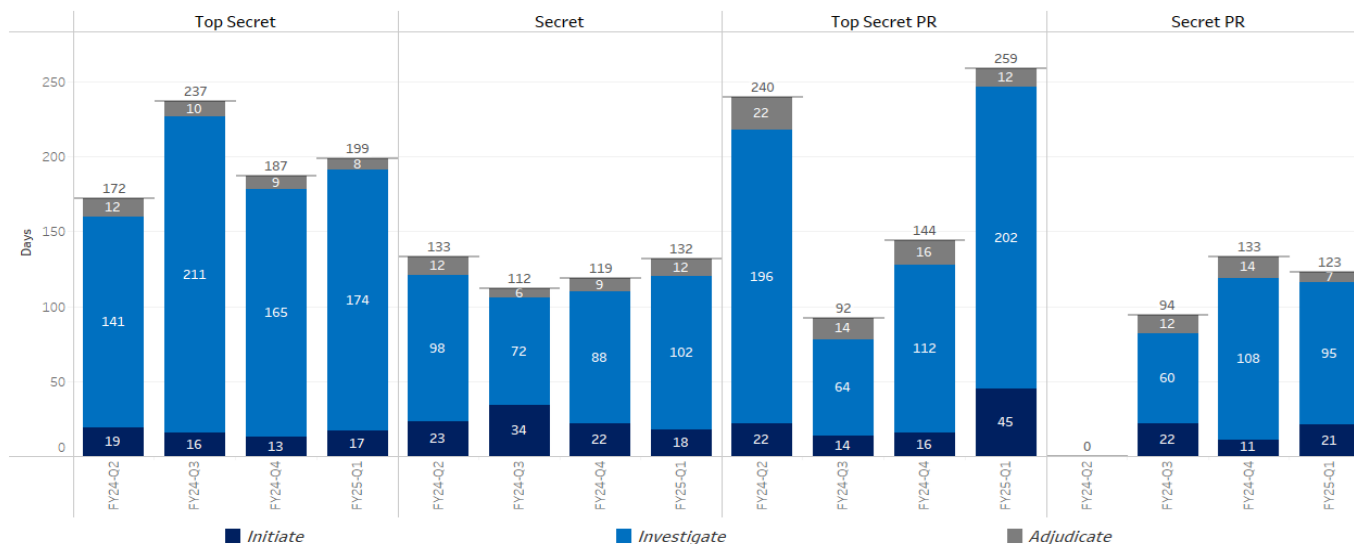
**Nuclear Regulatory Commission**

PERSONNEL SECURITY BRANCH  
DIVISION OF FACILITIES AND SECURITY  
OFFICE OF ADMINISTRATION  
U.S. NUCLEAR REGULATORY COMMISSION



# Quarterly NRC Timeliness Performance Metrics

Average Days for Fastest 90% of Reported Clearance Decisions Made

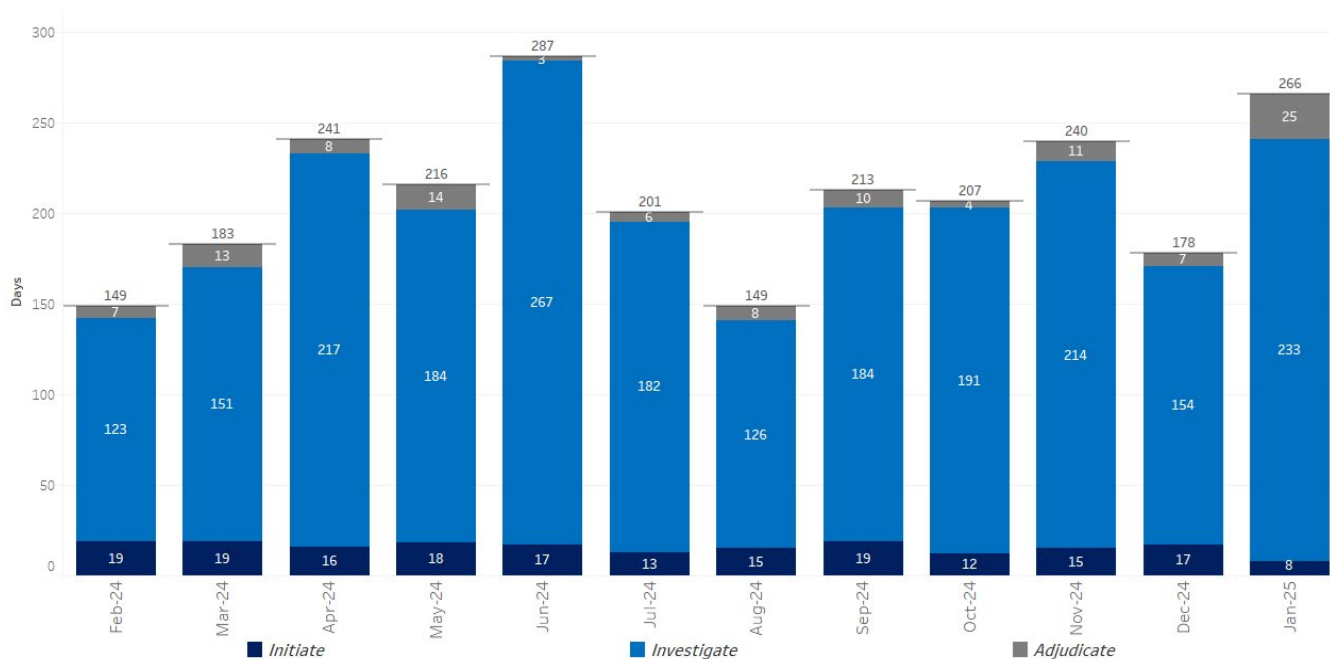


Total Adjudications Reported

	Top Secret	Secret	Top Secret PR	Secret PR
FY24-Q2	33	78	1	0
FY24-Q3	30	125	12	5
FY24-Q4	38	116	12	6
FY25-Q1	21	94	6	5

# Quarterly NRC Timeliness Performance Metrics

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

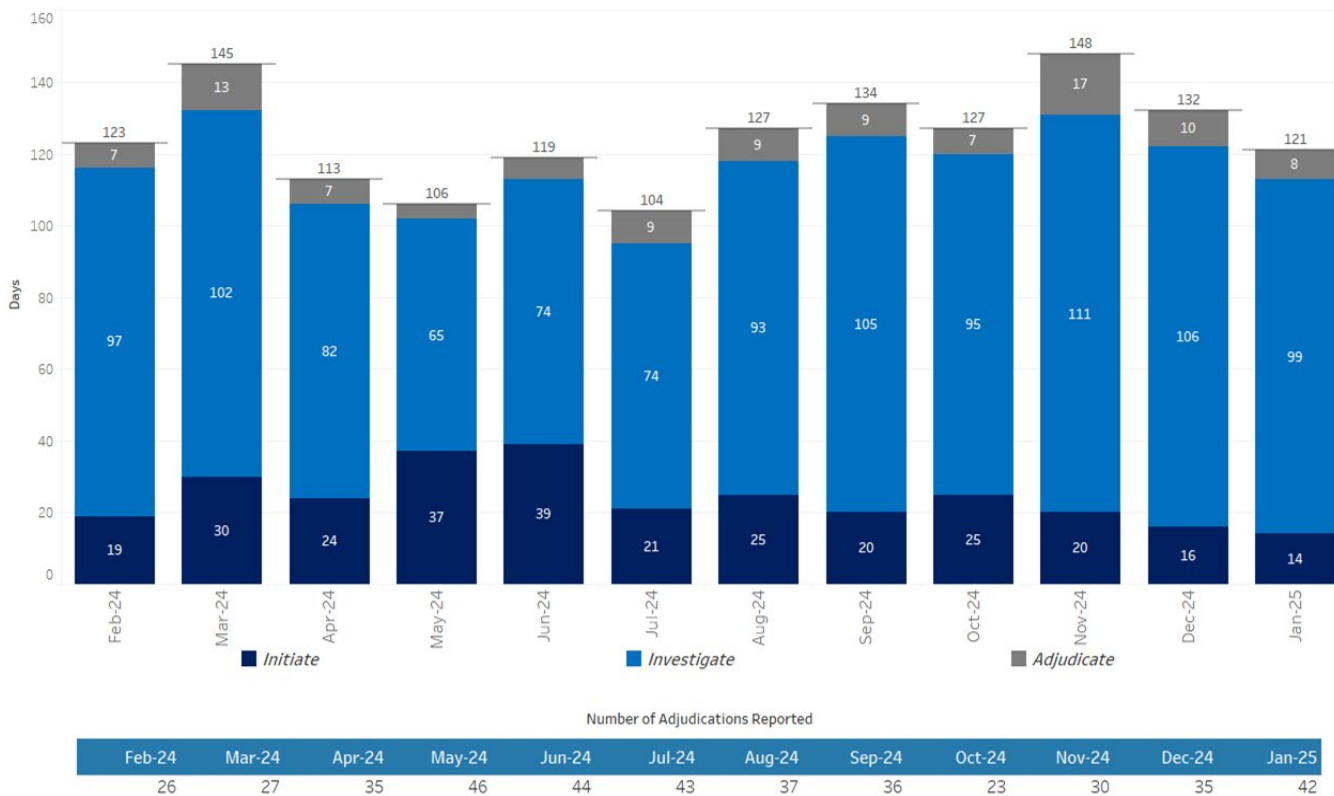


Number of Adjudications Reported

Feb-24	Mar-24	Apr-24	May-24	Jun-24	Jul-24	Aug-24	Sep-24	Oct-24	Nov-24	Dec-24	Jan-25
8	12	10	14	6	7	11	19	8	7	4	14

# Quarterly NRC Timeliness Performance Metrics

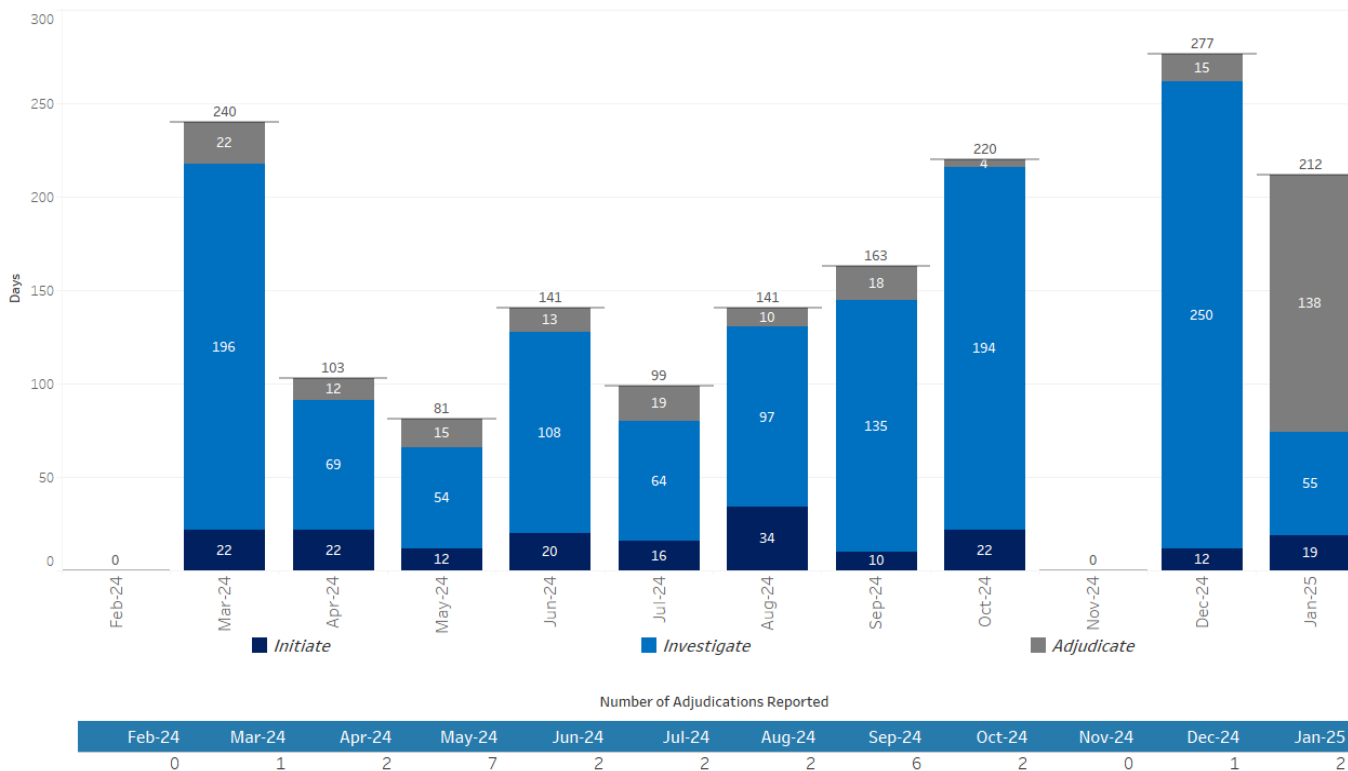
## Monthly Timeliness for Fastest 90% of Initial Secret (T3) Security Clearance Decisions





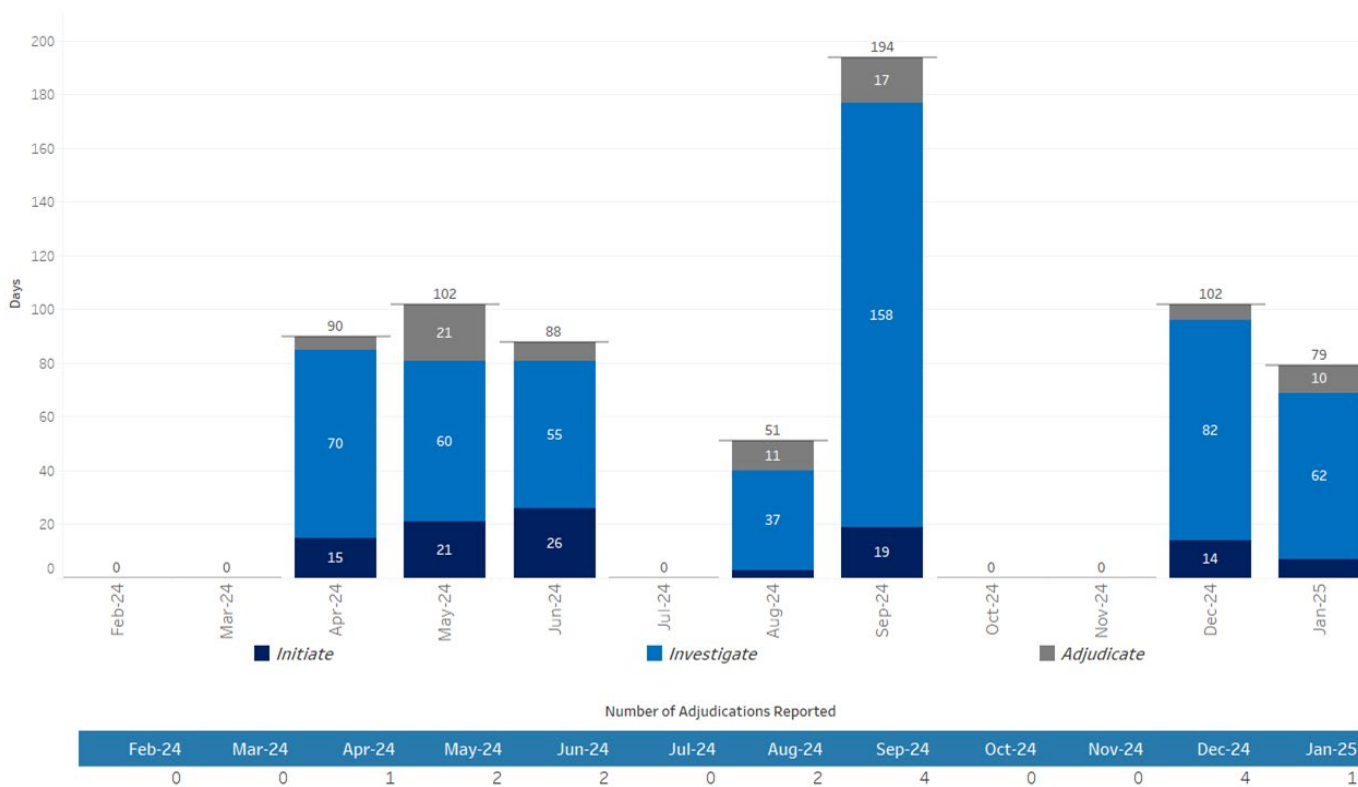
# Quarterly NRC Timeliness Performance Metrics

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



# Quarterly NRC Timeliness Performance Metrics

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



# WORKING GROUPS



DCSA NSCO :  
David Scott



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION

# DCSA NISP CYBERSECURITY OFFICE (NCSO)

**DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY**

**DAVID SCOTT**  
NISP CYBERSECURITY OFFICE  
INDUSTRIAL SECURITY DIRECTORATE





# FY25 Implemented NISP eMASS Enhancements

- NISP eMASS Release 5.11.2 deployed October 2024.
- The highlights of the NISP specific enhancements included:
  - Added system information fields to support facility categorization (i.e., “Workstations” and “Servers” system-level fields)
  - Several authorization workflow upgrades to further streamline the assessment and authorization process (updated workflow notices, authorization workflow decision document preview, and enhanced historical workflow editing capability)
  - Added filtering options and fields within executive/system-level dashboards and system search functions
  - Improved functionality within existing modules (System POA&M, National Security System Determination Questionnaire, System Implementation Plan, and System Relationships)



# FY25 Planned NISP eMASS Enhancements

- The FY25 planned enhancements include:
  - Enabling an Assets Module to track software and hardware
  - Implementing custom workflows (ISA, PDS, Change Request, Admin Update)
  - Displaying Assignment Values and Custom DCSA Guidance in Test Result Template.
  - Utilizing the developed NIST SP 800-53 Revision 5 migration capability to improve test results requirements
  - Continue refining authorization workflows by including additional warning message, priority tracking, and acknowledgements
  - Developing a MOU registration type to create a repository and track processing with metric capabilities.
  - Displaying Control Counts per Control Approval Chain (CAC) Stage on System > Dashboard.
  - Streamlining fields, sections, and modules to better meet NISP specific guidance.





# NIST SP 800-53 R5

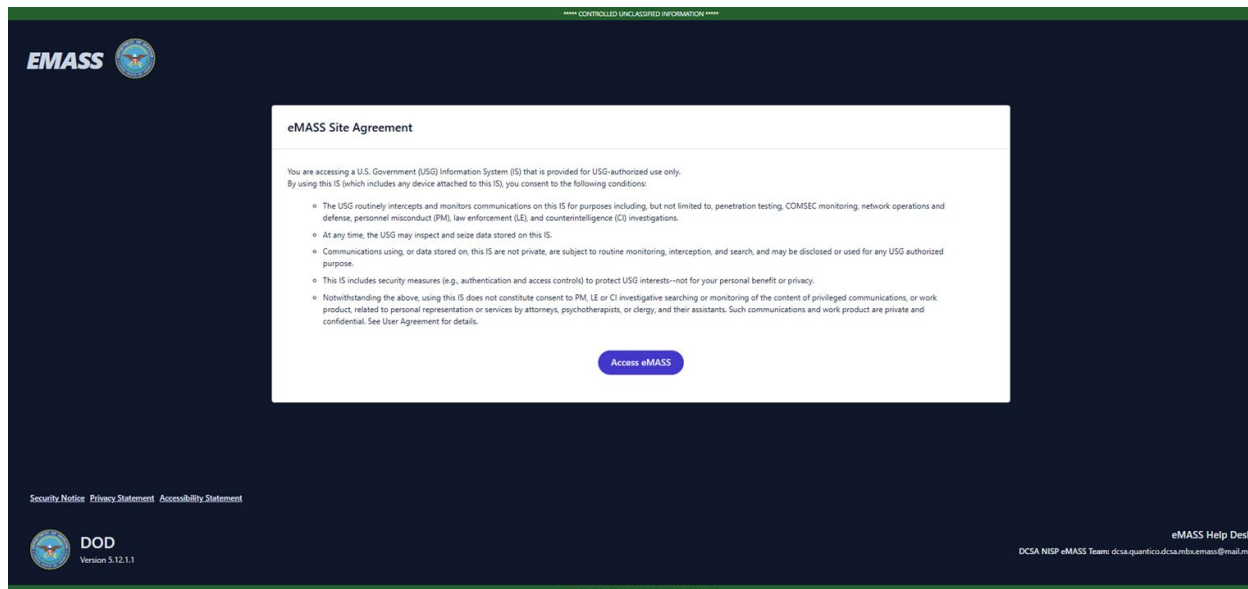
## When will NISP eMASS transition to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 security control set?

- Prior to the NISP eMASS being updated to include revision 5 security controls, DCSA must revise organizational guidance, including the associated baselines and overlays.
- NIST SP 800-53 Revision 4 remains the current security control set to align with the existing DCSA Assessment and Authorization Process Manual (DAAPM) Appendix A and B.
- DCSA is unable to provide an estimated time of transition due to the existing dependencies. As we get closer to a target date, Industry will be notified, and a transition plan provided.



# NISP eMASS Resources

- NISP eMASS Release Notes, guides, templates, and job aids are available on the NISP eMASS HELP page:  
<https://nisp.emass.apps.mil/App/Help/Home>



- Monitor the NISP eMASS Announcements.
- Contact the DCSA NISP eMASS Team:  
[dcsa.quantico.dcsa.mbx.emass@mail.mil](mailto:dcsa.quantico.dcsa.mbx.emass@mail.mil)





# National-Level Metrics

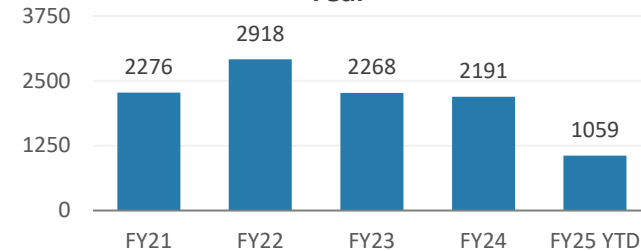
## NISP Cybersecurity Office: Overview

### Current Number of Active NISP Systems

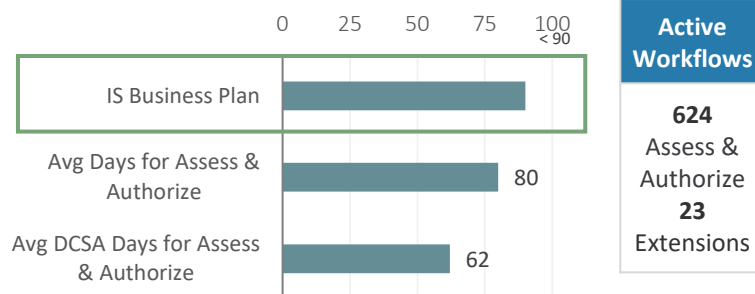
National: 4,905

<b>Central:</b>	<b>Eastern:</b>
1,205 (24.6%)	1,318 (26.8%)
<b>Mid-Atlantic:</b>	<b>Western:</b>
962 (19.6%)	1,420 (29.0%)

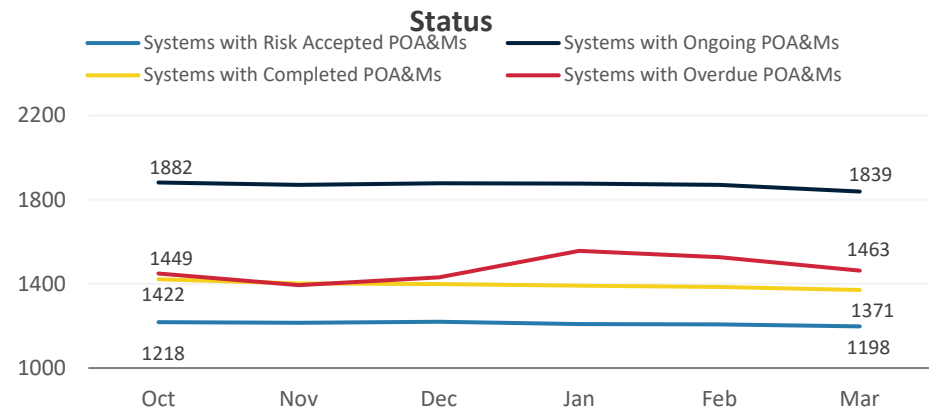
### Number of Authorizations Processed by Fiscal Year



### Average # of Days for NISP eMASS Authorization Decision



### FY25 System POA&M Status





# DAAPG v3.0 update

- Name change – DCSA Assessment & Authorization Process Guide
  - *Completed*
    - Internal Working Group led revision & updates to align with CNSS 1253 as appropriate
    - Updates to applicable references
    - Provide clarity to areas identified by industry & internal work force since previous addition
- Coordination process
  - Completed Informal coordination with NISA Working Group completed March 2024
  - In Process – formal coordination process
  - Transition & release – tbd

# WORKING GROUPS



**DCSA AVS :  
Donna McLeod**



**NISPPAC  
PUBLIC  
MEETING**

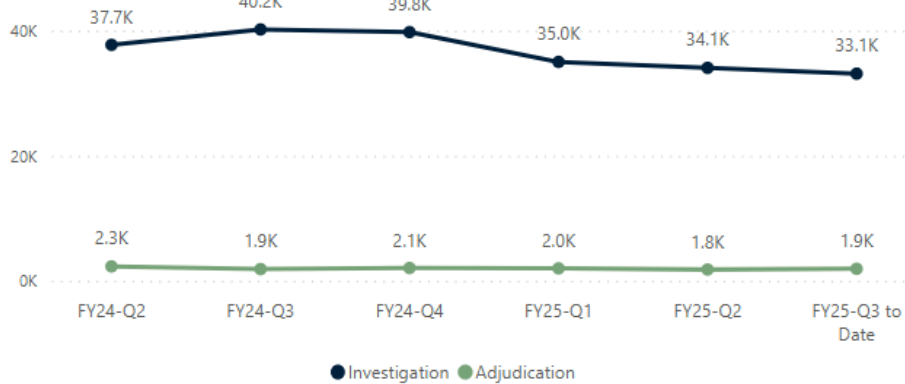
**MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION**



# DCSA INVENTORY & TIMELINESS | Industry

DoD-Industry Pending (as of 5 May)

includes T5/T3/T5R/T3R



DoD-Industry Pending by Case Type (as of 5 May)

## Investigation Inventory

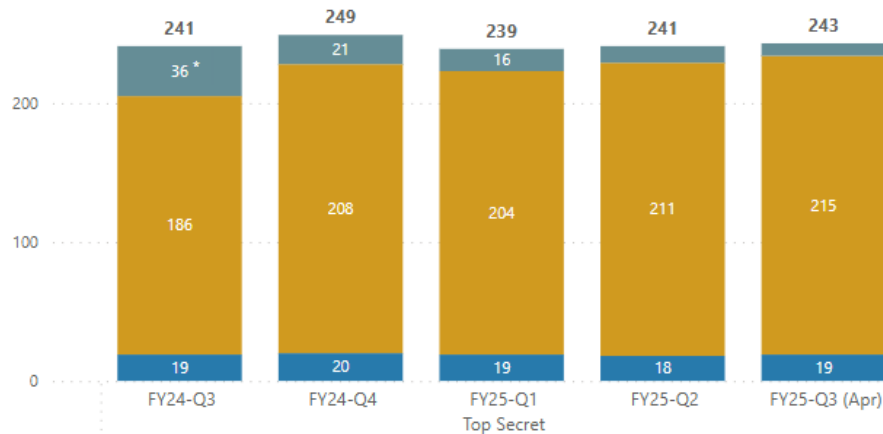
T5		T3	
FY24 End	Current	FY24 End	Current
21.1K	18.9K	18.5K	14.3K

## Adjudication Inventory

T5		T3	
FY24 End	Current	FY24 End	Current
0.5K	0.6K	1.1K	1.0K

Fastest 90% Timeliness - Initial Top Secret

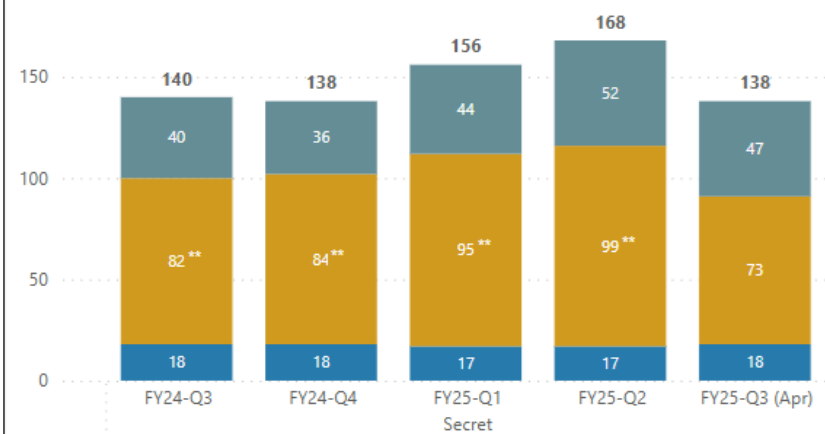
Initiate Investigate Adjudicate



\*DISS technical issue impacting ~440 Top Secret adjudications in FY24-Q3 resulted in a temporary spike in timeliness. Adjudication timeliness for unaffected cases averaged 31 days during FY24-Q3.

Fastest 90% Timeliness - Initial Secret

Initiate Investigate Adjudicate



\*\*Delays in FBI Name Checks have negatively impacted investigation timeliness over the past 12 months. Timeliness for unaffected cases was 78 days in FY24-Q2, 79 days in FY24-Q3 & FY24-Q4, 86 days in FY25-Q1, and 93 days in FY25-Q2.

# TOPIC BRIEFINGS



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION

# TOPIC BRIEFINGS



## DOHA : Perry Russell-Hunter



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION



# TOPIC BRIEFINGS



## ISOO : David Means



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION

# Controlled Unclassified Information (CUI)



Information Security Oversight Office (ISOO)

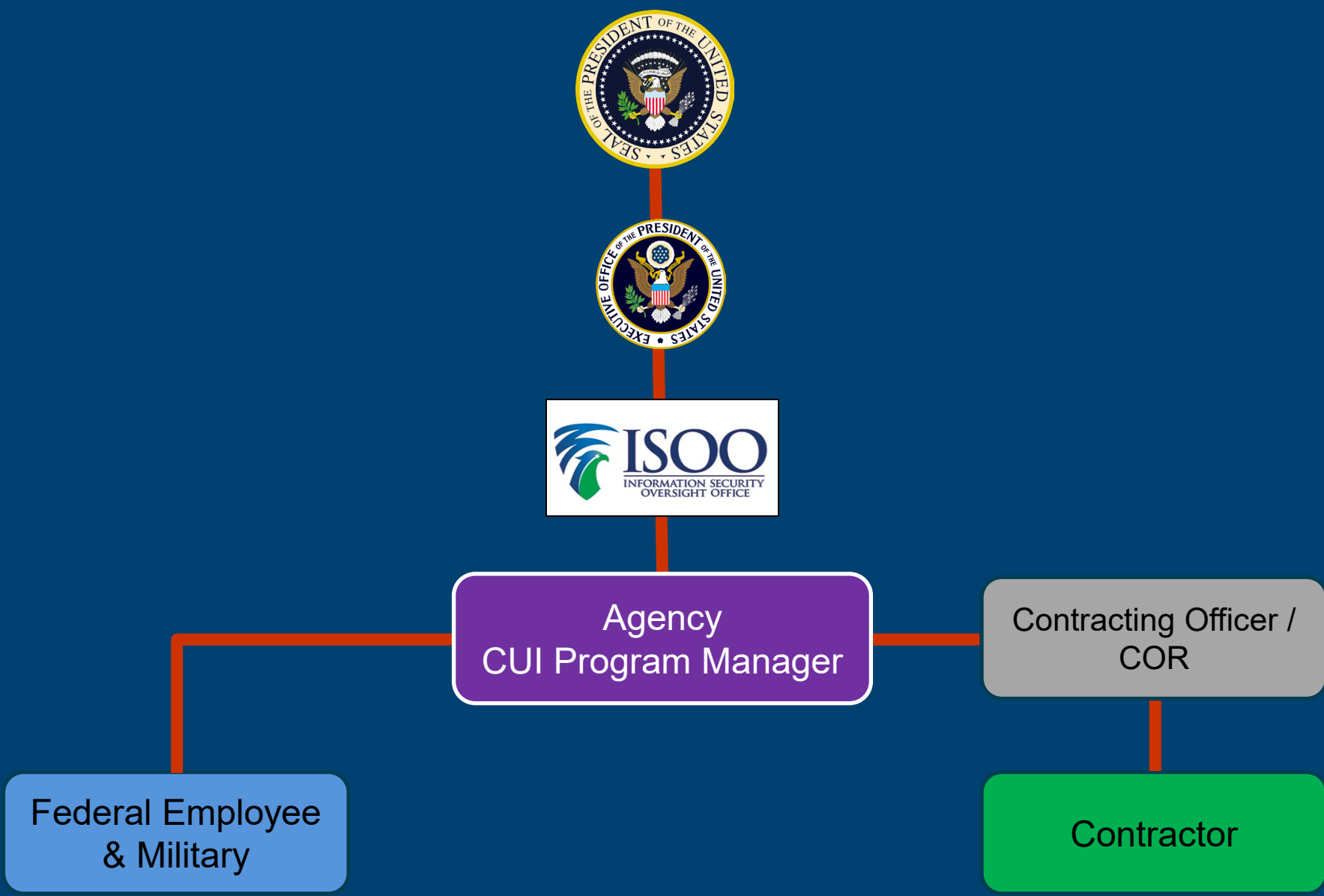


- Executive Order (EO) 13556
- 32 Code of Federal Regulations (CFR) 2002
- ISOO CUI Notices
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Rev. 3
- NIST SP 800-171A, Rev. 3

At a minimum, contracts must include provisions that state:

- *Specific* CUI handling requirements
- Process for CUI challenges
- Process for reporting misuse of CUI
- Penalties for misuse of CUI
- Requirement to comply with EO 13556, 32 CFR 2002 and CUI Registry

# Program Structure



[cui@nara.gov](mailto:cui@nara.gov)

# TOPIC BRIEFINGS



## CMMC : Stacy Bostjanick



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION



SLIDES ONLY  
NO SCRIPT PROVIDED

CLEARED  
For Open Publication

Apr 08, 2025

Department of Defense  
OFFICE OF PREPUBLICATION AND SECURITY REVIEW



# Cybersecurity Maturity Model Certification

Program Overview and Foreign Partner Integration into CMMC Ecosystem

May 27, 2025



## CMMC

**What:**

A consistent pre-award assessment methodology to determine whether a prospective contractor has implemented cybersecurity protections necessary to adequately safeguard DoD information.

**Why:**

To increase the cybersecurity posture of the DIB and better protect sensitive unclassified information.

**How:**

All defense contractors and subcontractors will show compliance with applicable security requirements through self-assessment or independent assessment, prior to contract award (excluding Commercial-Off-The-Shelf procurements).



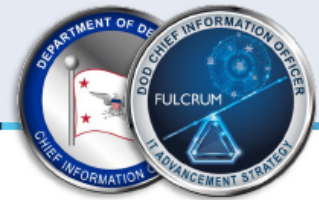


## Existing DoD Cybersecurity Requirements

- DFARS clause 252.204-7012 – **Effective Oct 2016 (to be implemented NLT Dec 2017)**
  - Safeguard DoD CUI that resides on or is transiting through a contractor/subcontractor internal information system or network by implementing NIST SP 800-171 at a minimum
  - Report cyber incidents that affect contractor/subcontractor ability to perform requirements designated as operationally critical
- DFARS Provision 252.204-7019 – **Effective Nov 2020**
  - Implement DFARS clause 252.204-7012 and have at least a Basic NIST SP 800-171 DoD Assessment that is current (i.e., not more than three (3) years old unless a lesser time is specified in the solicitation) posted in SPRS
- DFARS clause 252.204-7020 – **Effective Nov 2020**
  - Provide Government access when necessary to conduct or renew a higher-level Assessment
  - Include requirements of the clause in all applicable subcontracts and ensure applicable subcontractors can conduct and submit an Assessment

CMMC assesses whether a prospective DoD contractor has implemented these standards





## The CMMC Clause

- DFARS clause 252.204-7021
  - Relies on the requiring activity to identify the appropriate CMMC Status requirements based on the type of information to be processed, stored, or transmitted
  - Requires the contractor/subcontractor to:
    - Develop and update Artifacts and Deliverables per RFI/RFP
    - Conduct Self-Assessment or request a C3PAO or DIBCAC to perform a CMMC Certification Assessment, depending on the sensitivity of the data on the contractor's or subcontractor's information system
    - Complete annual affirmation of continued compliance in SPRS
    - Flow-down the DFARS clause 252.204-7021 to subcontractors

DoD is updating Title 48 CFR (the DFARS) to include revised CMMC Requirements



# U.S. Federal CUI Safeguarding Requirements

## The DoD follows a strict set of safeguarding requirements

The DoD adheres to the federal CUI safeguarding standard, as outlined in 32 CFR Part 2002, and implements NIST SP 800-171 requirements via DFARS 252.204-7012

- **The DoD follows the federal CUI safeguarding standard**
  - 32 CFR Part 2002 establishes federal policy for designating, handling, and decontrolling information that qualifies as CUI
    - § 2002.14: Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on nonfederal information systems
- **32 CFR Part 170 codifies DoD policy for verifying compliance with NIST SP 800-171 through CMMC assessment**
  - Compliance will be assessed in accordance with new contractual requirements, as proposed in 48 CFR
- **Countries may have their own national standards, creating a need to:**
  - Compare the foreign standard against NIST SP 800-171 to identify requirement gaps ("crosswalk")
  - Meet NIST SP 800-171 requirement gaps for DoD procurements containing CUI safeguarding requirements



# Compliance with DoD Cybersecurity Requirements

## Foreign partners can integrate into the existing CMMC Program

Foreign partners can participate in the accreditation process, submit self-assessments, and comply with DoD cybersecurity requirements to participate in DoD procurements

- DoD's CUI safeguarding requirements and associated compliance assessments apply uniformly to all contractors
- Accordingly, the DoD implements the following standards:
  - FAR 52.204-21 is the USG's basic safeguarding requirement; CMMC Level 1 self-assessment will be required
  - DFARS clause 252.204-7012 is DoD's covered defense information safeguarding requirement; various assessments are required by DFARS clauses 252.204-7019, 7020, and 7021

## Foreign partners must meet the same cybersecurity requirements as U.S. companies

Foreign companies will submit self-assessments, as required, and must comply with DoD cybersecurity requirements to participate in DoD procurements

- CMMC assessment requirements are codified in 32 CFR Part 170 and provide for international compliance with and participation in the CMMC ecosystem
  - Foreign companies will submit self-assessments, as required
  - The CMMC Program does not prohibit foreign citizens from becoming CCAs or foreign companies from becoming authorized/accredited as C3PAOs
  - Companies may employ assessment services from any authorized/accredited C3PAO or CCA



# Participation in the CMMC Ecosystem

## Foreign partners must meet specific requirements to participate in the CMMC ecosystem

Foreign assessors must complete a Tier 3 background investigation or equivalent, pass the CAICO-managed CMMC assessor certification exam, and comply with ISO/IEC 17011:2017, 17020:2012, and ISO/IEC 17024:2012 standards

- Any organization that meets all requirements of 32 CFR § 170.9 can operate as a C3PAO
- Any individual that meets all requirements of 32 CFR § 170.11 or § 170.13 can act as a CCA or CCP, respectively
  - Foreign assessors must complete a Tier 3 background investigation or equivalent
  - Foreign assessors must complete and pass the CAICO-managed CMMC assessor certification exam
  - Foreign assessors can take CAICO provided training, or foreign partners may obtain CAICO training materials and blueprints to develop their own training
  - Foreign Assessors may be employed by U.S.-based or foreign C3PAOs

## The DoD recognizes a single CMMC Accreditation Body (CMMC AB)

- The CMMC AB can accredit U.S.-based or foreign candidate C3PAOs (when all requirements are met)
- 32 CFR Part 170 allows the CMMC AB to establish Mutual or Multilateral Recognition Arrangements with other accreditation, inspection, and personnel certification bodies, in accordance with ISO/IEC

## The CMMC Program is open to foreign participation

The CMMC Program does not prohibit foreign citizens from becoming CCAs or foreign companies from becoming authorized/accredited as C3PAOs

- In accordance with 32 CFR Part 170, DCMA's DIBCAC performs all CMMC Level 3 and candidate C3PAO Level 2 assessments
  - Foreign partners may participate jointly in DCMA DIBCAC on-site assessment activities



# CMMC Ecosystem



## DoD – DoD CIO CMMC PMO - § 170.6

- Provides oversight of the CMMC Program, to include the CMMC AB
- Develops and maintains the CMMC Model Overview, Assessment Guides, Scoping Guides, and Hashing Guide
- Scheme Owner for ISO/IEC Requirements
- Establishes DoD requirements of C3PAOs, CAICO, Assessors, and Instructors



## DoD - DCMA DIBCAC - § 170.7

- Conducts CMMC Level 2 Certification Assessments on C3PAOs
- Conducts CMMC Level 3 Certification Assessment on DIB
- Advises DoD CIO CMMC PMO



## C3PAOs – § 170.9

- ISO / IEC 17020
- Conducts CMMC Level 2 Certification Assessments on DIB contractors
- Employs Assessors
- Submits Assessment Report in eMASS
- Issues CMMC certificate to DIB contractor

DoD Contract

## CMMC AB - § 170.8

- Professionally staffed
- Managed by Board of Directors
- ISO / IEC 17011 Compliant
- Accredits C3PAOs
- Accredits CAICO



## CAICO - § 170.10



Agreements



## CMMC Certified Professionals, Assessors & Instructors – § 170.11, § 170.12 and § 170.13

- Certified by CAICO IAW ISO/IEC 17024



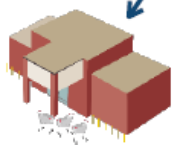


# CAICO



## CMMC Assessor and Instructor Certification Organization - § 170.10

- ISO/IEC 17024
- Certifies CMMC Certified Professionals, Assessors, and Instructors
- Defines knowledge areas required for CCPs, CCAs, and CCIIs with input from DoD
- QCs curriculum developed by ecosystem



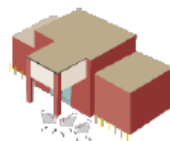
### Approved Publisher Partners

- Develops Training Materials



### Approved Training Providers

- Trains Certified Professionals
- Trains Assessors
- Trains Instructors
- In-person / Virtual / Hybrid



### Approved CMMC Exam Org

- Develops and administers Assessor and Instructor Certification Exams



# Foreign Partner Integration into CMMC – Course of Action 1 for CMMC L2

## COA 1: Existing Authorized C3PAOs

- Use existing Accreditation Body – Cyber AB
- Use existing CAICO
- Add new Foreign Partner CCPs and CCAs
  - Favorable Tier 3 Background Investigation
  - CCP: Complete Training & Pass Certification Exam
  - CCA:
    - Be a CCP
    - Complete CCA Training & Pass Certification Exam
  - Work Experience:
    - 1 year of Assessment or Audit Experience
    - 1 Foundational requirement aligned to at least the Intermediate Proficiency Level of the DoDM 8140.03

**Cyber AB – § 170.8**

- Professionally staffed
- ISO / IEC 17011 Compliant
- Accredits C3PAOs
- Accredits CAICO

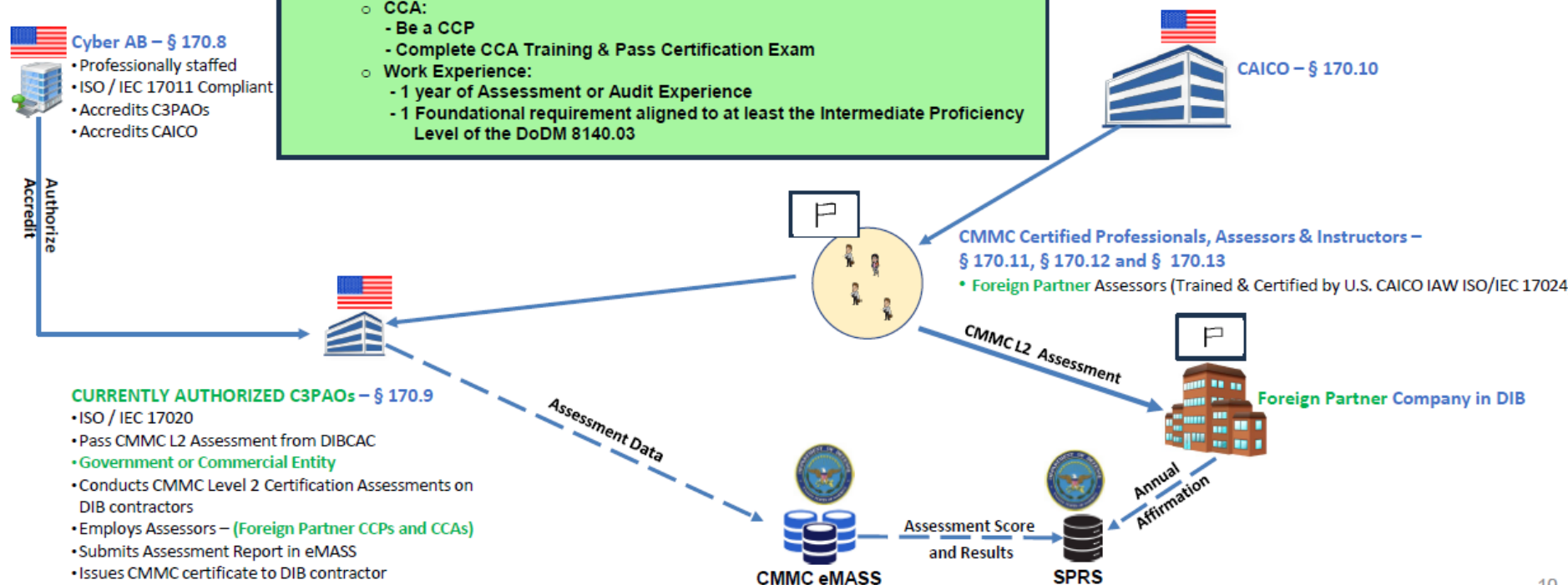
**CAICO – § 170.10**

**CMMC Certified Professionals, Assessors & Instructors – § 170.11, § 170.12 and § 170.13**

- Foreign Partner Assessors (Trained & Certified by U.S. CAICO IAW ISO/IEC 17024)

## CURRENTLY AUTHORIZED C3PAOs – § 170.9

- ISO / IEC 17020
- Pass CMMC L2 Assessment from DIBCAC
- Government or Commercial Entity
- Conducts CMMC Level 2 Certification Assessments on DIB contractors
- Employs Assessors – (Foreign Partner CCPs and CCAs)
- Submits Assessment Report in eMASS
- Issues CMMC certificate to DIB contractor






# Foreign Partner Integration into CMMC – Course of Action 2 for CMMC L2

## COA 2: New Authorized Foreign Partner C3PAOs P

- Use existing Accreditation Body – Cyber AB
- Use existing U.S. CAICO
- Add new Foreign Partner CCPs and CCAs
  - Favorable Tier 3 Background Investigation
  - CCP: Complete Training & Pass Certification Exam
  - CCA:
    - Be a CCP
    - Complete CCA Training & Pass Certification Exam
  - Work Experience:
    - 1 year of Assessment or Audit Experience
    - 1 Foundational requirement aligned to at least the Intermediate Proficiency Level of the DoDM 8140.03

 **Cyber AB – § 170.8**

- Professionally staffed
- ISO / IEC 17011 Compliant
- Accredits C3PAOs
- Accredits CAICO

Authorize  
Accredit

 **CAICO – § 170.10**

P **CMMC Certified Professionals, Assessors & Instructors – § 170.11, § 170.12 and § 170.13**

- Foreign Partner Assessors (Trained and Certified by U.S. CAICO IAW ISO/IEC 17024)

Assessment Data (Through CMMC PMO)

CMMC L2 Assessment

P **Foreign Partner Company in DIB**

### NEW Int'l Partner AUTHORIZED C3PAOs – § 170.9

- ISO / IEC 17020
- Pass CMMC L2 Assessment from DIBCAC
- Government or Commercial Entity
- Conducts CMMC Level 2 Certification Assessments on DIB contractors
- Employs Assessors – (Foreign Partner CCPs and CCAs)
- Submits Assessment Report in eMASS through CMMC PMO
- Issues CMMC certificate to DIB contractor

  
**CMMC eMASS**

Assessment Score  
and Results

  
**SPRS**

Annual  
Affirmation





# Foreign Partner Integration into CMMC – Course of Action 3 for CMMC L2

## COA 3: New Foreign Partner CMMC Ecosystem

- Create new Foreign Partner Accreditation Body IAW ISO 17011
- Mutual Recognition Agreement between Existing Cyber AB and new Foreign Partner CMMC AB
- Create new Foreign Partner C3PAO accredited by Foreign Partner CMMC AB
- Use existing U.S. CAICO
- Use Foreign Partner CCPs and CCAs Trained by U.S. CAICO approved ATP
  - Favorable Tier 3 Background Investigation
  - CCP: Complete Training & Pass Certification Exam
  - CCA:
    - Be a CCP
    - Complete CCA Training & Pass Certification Exam
  - Work Experience:
    - 1 year of Assessment or Audit Experience
    - 1 Foundational requirement aligned to at least the Intermediate Proficiency Level of the DoDM 8140.03

### Cyber AB – § 170.8

- Professionally staffed
- ISO / IEC 17011 Compliant
- Accredits C3PAOs
- Accredits CAICO

### Foreign Partner CMMC AB – § 170.8

- Professionally staffed
- ISO / IEC 17011 Compliant
- Accredits C3PAOs
- Accredits CAICO

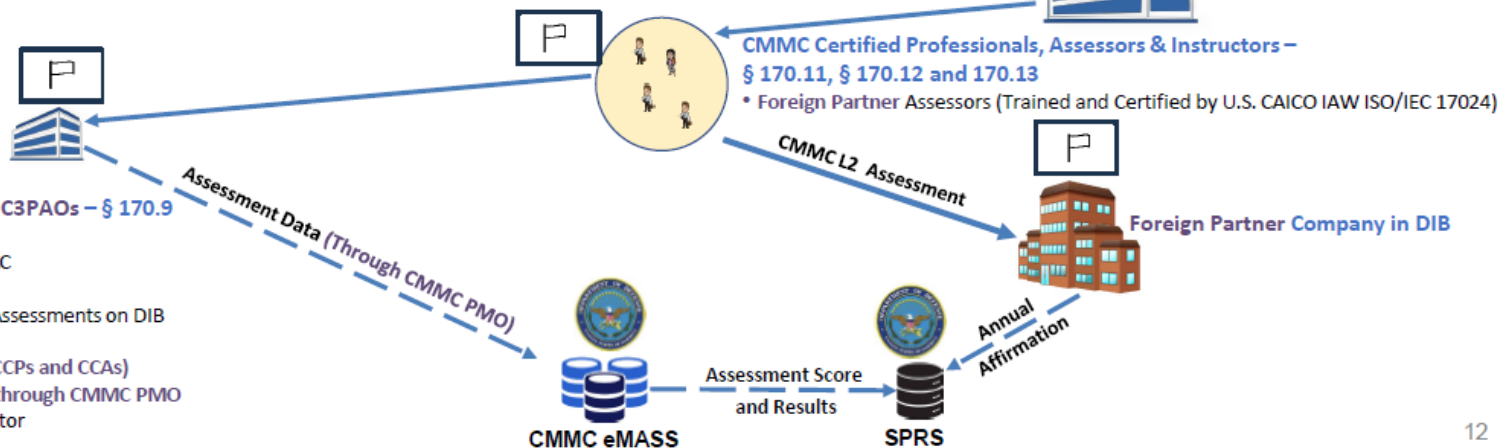
### CAICO – § 170.10

### CMMC Certified Professionals, Assessors & Instructors – § 170.11, § 170.12 and 170.13

- Foreign Partner Assessors (Trained and Certified by U.S. CAICO IAW ISO/IEC 17024)

### NEW Foreign Partner AUTHORIZED C3PAOs – § 170.9

- ISO / IEC 17020
- Pass CMMC L2 Assessment from DIBCAC
- Government or Commercial Entity
- Conducts CMMC Level 2 Certification Assessments on DIB contractors
- Employs Assessors – (Foreign Partner CCPs and CCAs)
- Submits Assessment Report in eMASS through CMMC PMO
- Issues CMMC certificate to DIB contractor





# Backups



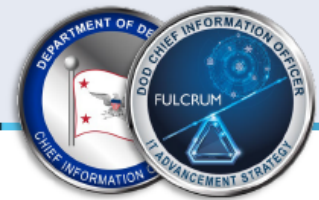
## Acronym Glossary

Acronym	Meaning
AB	Accreditation Body
CAICO	Cybersecurity Assessor and Instructor Certification Organization
CIO	Chief Information Officer (DoD)
CFR	Code of Federal Regulations
CMMC	Cybersecurity Maturity Model Certification
CCPs/CCAs/CCIs	CMMC Certified Professionals/Assessors/Instructors
C3PAO	Certified Third-Party Assessment Organization
CUI	Controlled Unclassified Information
DCMA	Defense Contract Management Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
DoD	Department of Defense
eMASS	Enterprise Mission Assurance Support Service



## Acronym Glossary Cont'd

Acronym	Meaning
EO	Executive Order
FAR	Federal Acquisition Regulation
FAQ	Frequently Asked Question
FedRAMP	Federal Risk and Authorization Management Program
FCI	Federal Contract Information
FIPS	Federal Information Processing Standards
IAW	In Accordance With
IG	Inspector General
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
MFA	Multi-Factor Authentication
NDAA	National Defense Authorization Act



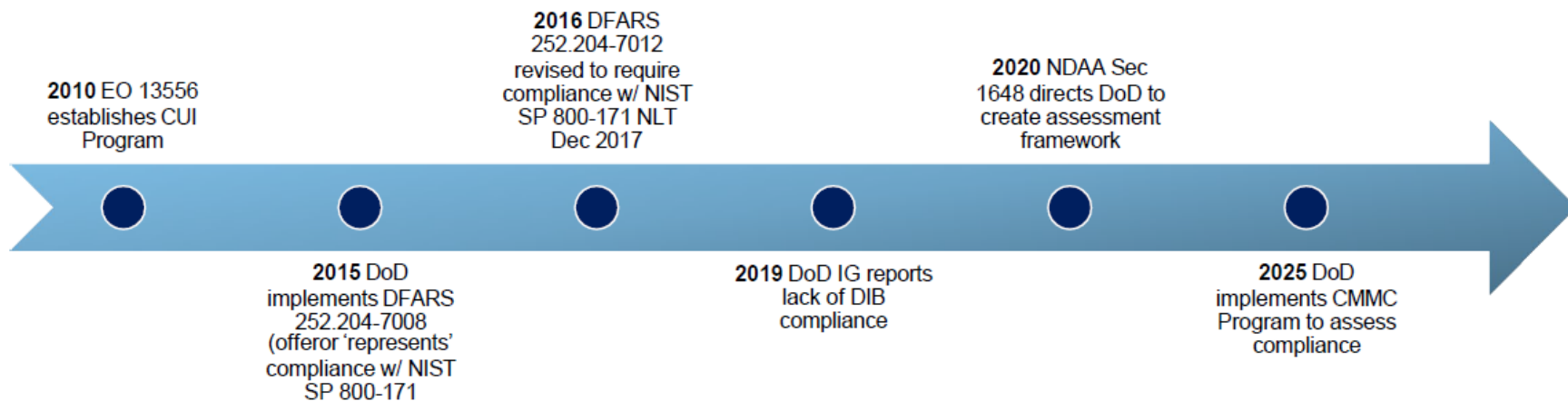
# Acronym Glossary Final

Acronym	Meaning
NIST	National Institute of Standards and Technology
NLT	No Later Than
POA&M	Plan of Action and Milestones
PMO	Program Management Office
Rev	Revision
RFI	Request for Information
RFP	Request for Proposal
SP	Special Publication
SPRS	Supplier Performance Risk System
QC	Quality Check



# CMMC Program Overview and History

The CMMC Program helps ensure that DoD contractors and subcontractors comply with DoD requirements to safeguard FCI and CUI.





## Safeguarding FCI and CUI

### Safeguarding Requirements for Nonfederal Information Systems

#### FCI

- Information that is not marked as public or for public release and is not designated as CUI
- Defined in FAR 52.204-21
- Minimum safeguarding requirement: 48 CFR 52.204-21

#### CUI

- Information that is marked or identified as requiring safeguarding in the DoD CUI Program
- Defined in 32 CFR Part 2002
- Minimum safeguarding requirement: NIST SP 800-171

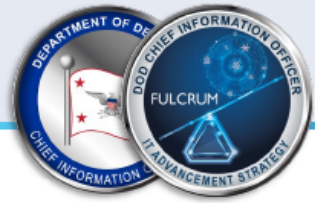


# Revised CMMC Framework Requirements

CMMC Model		
	Model	Assessment
<b>LEVEL 3</b>	<b>134</b> requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172)	<ul style="list-style-type: none"> <li>DIBCAC assessment every 3 years</li> <li>Annual Affirmation</li> </ul>
<b>LEVEL 2</b>	<b>110</b> requirements aligned with NIST SP 800-171 r2	<ul style="list-style-type: none"> <li>C3PAO assessment every 3 years, or</li> <li>Self-assessment every 3 years for select programs.</li> <li>Annual Affirmation</li> </ul>
<b>LEVEL 1</b>	<b>15</b> requirements aligned with FAR 52.204-21	<ul style="list-style-type: none"> <li>Annual self-assessment</li> <li>Annual Affirmation</li> </ul>

When specified in a solicitation, all CMMC requirements must be met prior to award





## CMMC Alignment to NIST SP 800-171 Revisions

- DoD followed federal rulemaking guidelines when aligning CMMC assessment requirements to NIST SP 800-171 **Rev 2**.
- Defense contractors can implement NIST SP 800-171 Rev 3, but must comply with **Rev 2 requirements not covered in Rev 3** to meet CMMC assessment requirements.
- DoD will incorporate Rev 3 with future rulemaking.





## Existing DoD Cybersecurity & Assessment Requirements

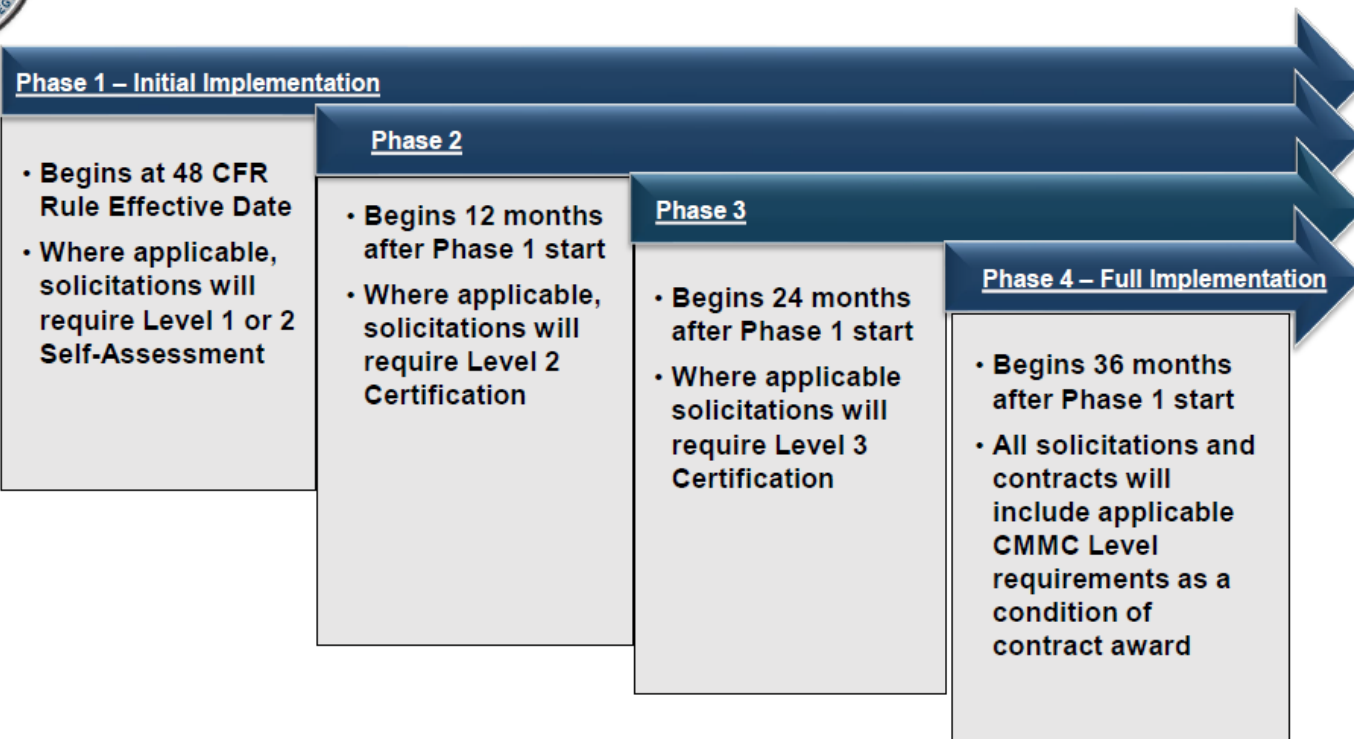
### Compliance with DoD cybersecurity requirements is mandatory

Contractors must comply with DFARS clauses 252.204-7012, 252.204-7019, 252.204-7020, and 252.204-7021 to participate in DoD procurements containing CUI safeguarding requirements.

- DFARS clause 252.204-7012 – **Effective Oct 2016**
  - Provide adequate security on covered contractor information systems (i.e., implement NIST SP 800-171 “as soon as practical, but NLT Dec 31, 2017” on systems that process, store, or transmit covered defense information)
  - Report cyber incidents that affect covered contractor information systems or covered defense information residing therein, or that affects ability to perform operationally critical support requirements identified in the contract
- DFARS Provision 252.204-7019 – **Effective Nov 2020**
  - Advises offerors subject to NIST SP 800-171 requirements to have a current NIST SP 800-171 DoD Assessment on record (in SPRS) to be considered for award
  - Current is defined as not more than three (3) years old unless a lesser time is specified in the solicitation
- DFARS clause 252.204-7020 – **Effective Nov 2020**
  - Provide access to facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment (if necessary)
  - Include requirements of the clause in all applicable subcontracts and ensure applicable subcontractors have the results of a current assessment posted in SPRS prior to awarding a subcontract
- DFARS clause 252.204-7021 (Proposed CMMC clause) – **Published for public comment Aug 2024, Effective TBD**
  - Provides for the assessment of contractor implementation of the above applicable security requirements



# Phased Implementation of CMMC Requirements



In some procurements, DoD may implement CMMC requirements in advance of the planned phase

# DISCUSSION



ISOO :  
Jennifer May



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION

# CLOSING REMARKS



ISOO :  
Michael Thomas



NISPPAC  
PUBLIC  
MEETING

MAY 28, 2025  
NATIONAL ARCHIVES &  
RECORDS ADMINISTRATION