Information Security Oversight Office

Protect • Inform • Assess

Agenda

- Welcome, Introductions, and Administrative Matters
- Reports and Updates
  - Industry
  - Department of Defense (DoD)
  - Defense Counterintelligence and Security Agency (DCSA)
  - Office of the Director of National Intelligence (ODNI)
  - Department of Homeland Security (DHS)
  - Department of Energy (DOE)
  - Nuclear Regulatory Commission (NRC)
  - Central Intelligence Agency (CIA)
  - Underwriters Laboratories (UL)
- Working Group Updates
  - DOE
  - NRC
  - DCSA Cyber
  - DCSA Adjudication and Vetting Services (AVS)
- Defense Office of Hearings and Appeals (DOHA)
- General Discussion, Remarks, and Adjournment

Opening Remarks
ISOO

Reports & Updates

Industry Update

Ike Rivers (NISPPAC Spokesperson)

National Industrial Security Program Policy Advisory Committee (NISPPAC)

NISPPAC Industry Updates

November 2024

THANK YOU
Tracy & Derek!!!

Industry's NISPPAC Current Members

WELCOME
LaToya & Charlie

Isaiah "Ike" Rivers
Institute for Defense Analyzes (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

Dr. Douglas Edwards
Raytheon Technologies
2023 - 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

Industry Association Support

WELCOME
Mary & Jim

Memorandum of Understanding (MOU) Industry Association Security Representatives	
Heather Sims	Aerospace Industries Association (AIA)
Jonathan Fitz-Enz	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)
Marc Ryan	Professional Services Council (PSC)
Rosie Borrero-Jones	Community Association for Information Systems Security Working Group (CAISSWG)

Key Issues/Concerns: Physical Security

➢ **Tier 1 concerns**

- Lack of consistent *policy* on a strategy for implementation of ICD705/Tempest across **all of Government** for SCIFs and SAPFs.
- Flexibility to implement plan for compliance within a *reasonable* timeframe – **progress**
- Continued understanding of the threat – **good progress**
- Data – understanding the magnitude of the problem

➢ **Tier 2 concerns**

- Adequate trained Government staff to implement guidance (CTTA)
- Acceptance of use of tests conducted by the company as basis of POAM
- Funding for modifications - direct charge or contractor funded
- Supply chain support
- Impact to mission during renovations

Key Recent Milestones

- *12 January 2024 - meeting w/SSCI*
- *31 January 2024 - threat briefing at NSA*
- *20 March 2024 - comments to SSCI on Draft Provision of ICD705*
- *12 March 2024 -threat briefing provided by NSA to key Industry members*
- *13 March 2024 - ISOO approval of new Working Group*
- *1 May 2024 - first meeting of the Working Group*
- *6 May 2024 - threat briefing by IC to industry at AIA/NDIA*
- 9 Sep 2024 – threat briefing by NSA to industry at ISWG. IC Directors strategy discussion
- 25 Sep 2024 – Working group meeting
- 6 October 2024 – AIA/NDIA engagement
- December 2024 – ISOO Working Group Meeting

Current State

- NSA taken “lead” with threat
  - Government “owns” distribution of threat information
- Multiple conversations with other IC members
  - CIA, NRO, DIA, ODNI, FBI
- DIB transition strategy created/socialized
- Data collection important to understand magnitude
- Agreement to review at enterprise level of companies
- Realistic expectations

Next Steps

Q3 2024	Q4 2024	2025
✓ Present Strategy to IC Security Directors (9 Sep) ✓ Discuss and Align Goals & Strategy with IC Security Directors	☐ Present strategy to Defense SAP Security Directors ☐ Discuss and Align Goals & Strategy with SAP & IC Security Directors (Working Group Meeting)	☐ Q1: Data Picture Established by Industry ☐ Q2: Critical Area Prioritization ☐ Q3: POAMs Established ☐ Q4: Strategy Review

PROPOSED DIB Classified Area Transition Strategy

16 Aug 2024

Expectations: All classified areas must be ICD 705 compliant

- DoD & IC allowed risk-balanced exceptions to ICD 705 standards
- Increased risk reduces exception allowances
- Customers are shifting to full compliance requirements
- Limited synchronization for implementing this shift

Goal: Synchronized transition process

- Centrally managed
- Informed by threats
- Risk-balanced mitigations
- Reasonable timelines

Strategy

Drive Efficiencies through Data Sharing & Management

Collect classified area data and discuss initial risk categorization with customers

Understand Enterprise Picture

Optimize Area via Future-Proofing

Analyze & reduce critical area footprint. Recommend mitigation opportunities

Reduce Critical Area Footprint

Establish Standardized Building Practices & Streamlined Processes

Standardize and Streamline SCIF build standards. Simplify procurement

Deliver Classified Area Playbooks

Synchronize National Security Community

Develop and deliver synchronized messaging of a risk mitigation approach to the customer community

Establish Stability & Reciprocity

Visualize Enterprise Picture → Identify & Reduce "Critical Area" Footprint → Establish Plans to mitigate risks at Critical Areas → Bring critical areas into compliance

Industry Topics

All CSA/CSOs

- SF 328 and Section 845
- Inquiry on Upcoming Policy Releases
- Physical Security and Continued Efforts for Consistency for 705/TEMPEST Compliance
- SCIF Escort –Potential Reciprocity for SCIF Escort during SCIF Buildouts

Department of Defense (DoD)

- Inquiry on any Feedback on the comments provide from Industry NISPPAC to the DoD Special Access Program (SAP) Manual Draft
- CUI/CMC - Implementation across DoD and IC

Defense Counterintelligence and Security Agency (DCSA)

- New Security Rating Scorecard
- Senior Management Officials (SMOs)/Designated Official (DOs) Job Aid
- Inquiry on possible Industrial Security Letter (ISL) for SMOs/DOs/Insider Threat
- Entity Vetting (FCL & FOCI) Backlog Update, Request for Metrics
- Investigation Timelines
- NBIS 36 Month Road Map and Industry Dual System Use Requirement (NBIS and DISS)

Office of the Director of National Intelligence (ODNI)

- Information Sharing and Overhead Billet Policies
- TORIS
- Inquiry on Potential Policies Impacting Industry

DoD Update

Jeff Spinnanger

(no slides)

DCSA Update

Various Speakers

(no slides)

ODNI Update

Lisa Perez

(no slides)

DHS Update

Rich Dejausserand

(no slides)

DOE Update

Jaime Gordon

(no slides)

NRC Update

Mike England

(no slides)

CIA Update

Jennifer

(no slides)

UL Briefing

John McMahon

(no slides)

Working Group Updates

DOE
Tracy Kindle

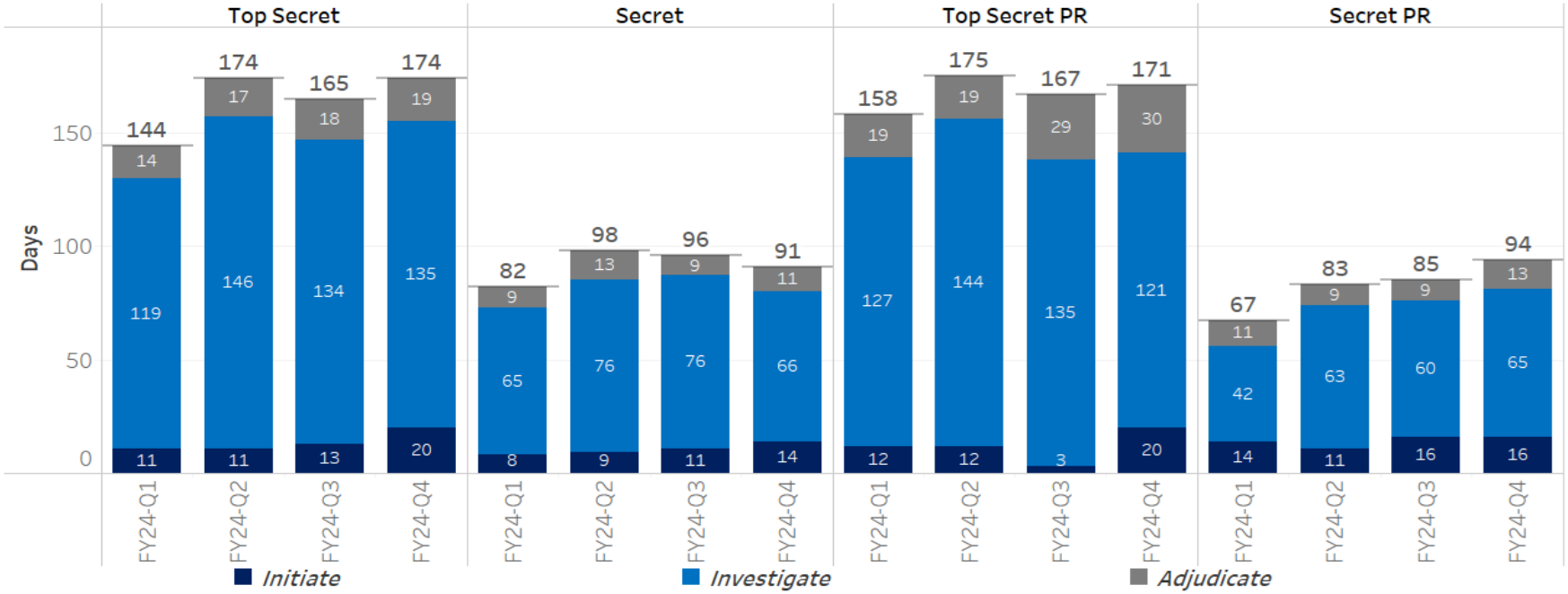
Workload & Timeliness Performance Metrics

Department of Energy

*Metrics provided by Defense Counterintelligence and Security Agency

Quarterly DOE Timeliness Performance Metrics

Average Days for Fastest 90% of Reported Clearance Decisions Made



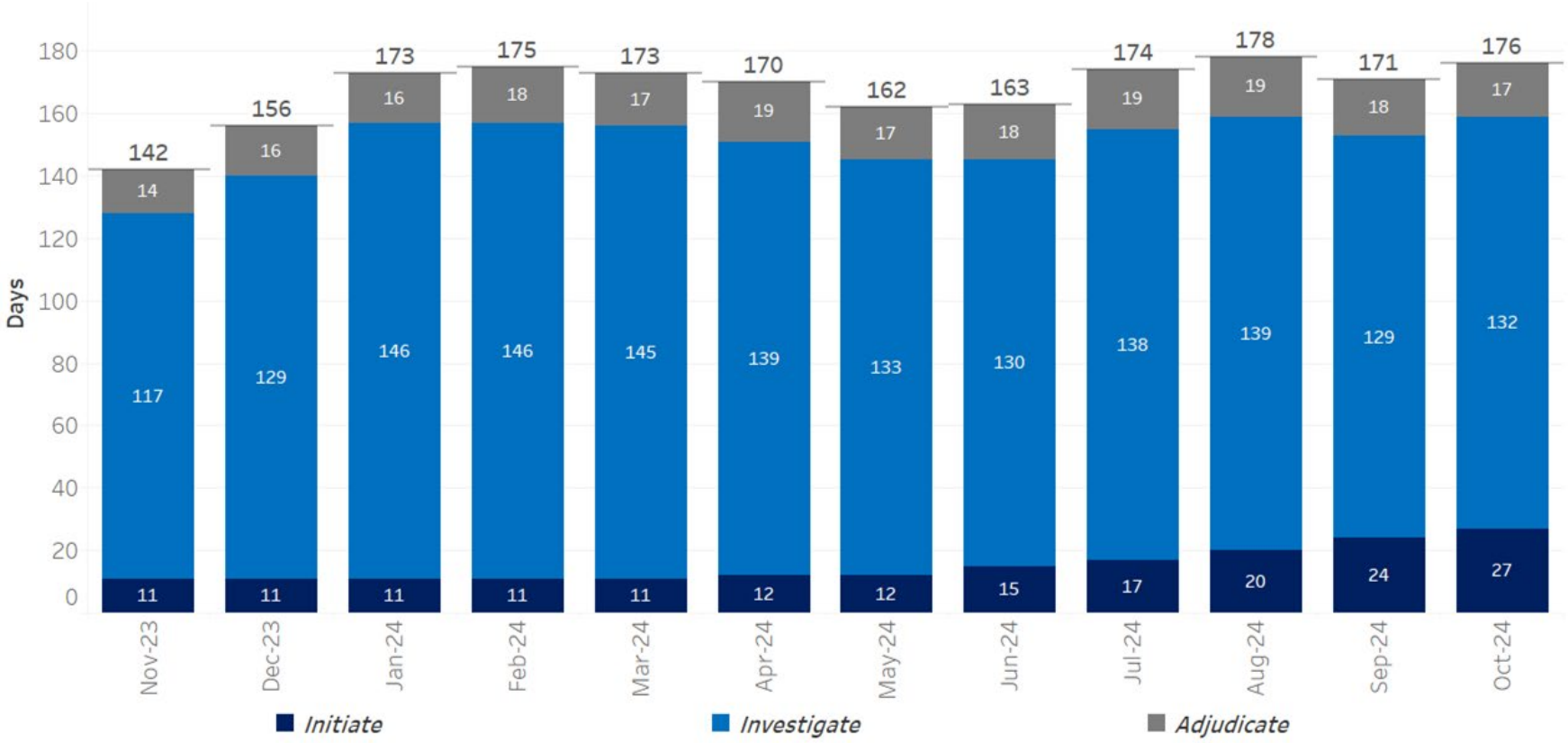
Total Adjudications Reported

	Top Secret	Secret	Top Secret PR	Secret PR
FY24-Q1	2,227	568	271	74
FY24-Q2	2,725	542	251	80
FY24-Q3	2,633	550	312	112
FY24-Q4	2,070	481	304	162

Data representative of DOE Contractor investigations

UNCLASSIFIED

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

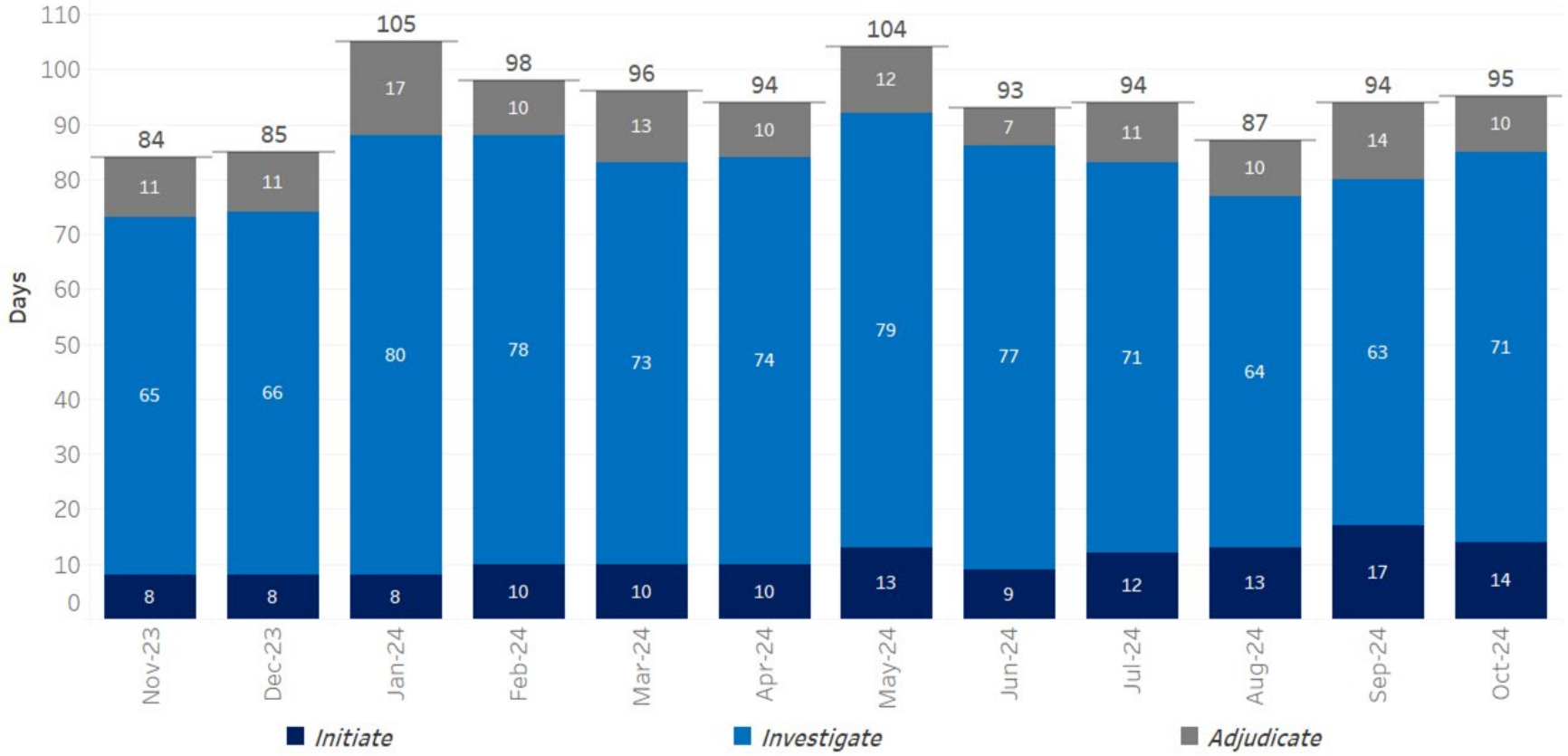


Number of Adjudications Reported

Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	Jul-24	Aug-24	Sep-24	Oct-24
847	726	997	879	849	970	969	694	775	630	665	698

Data representative of DOE Contractor investigations

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

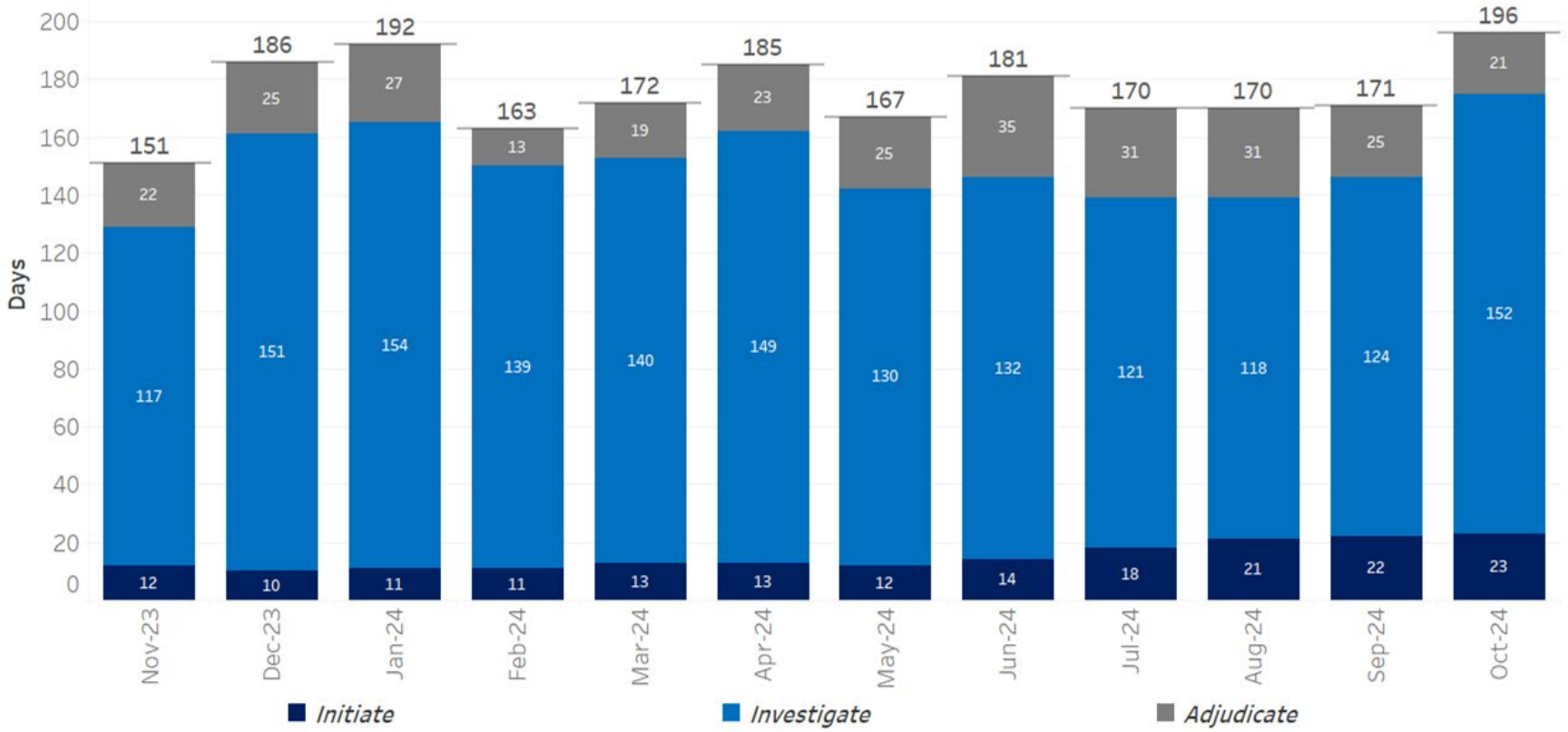


Number of Adjudications Reported

Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	Jul-24	Aug-24	Sep-24	Oct-24
161	178	176	191	175	215	162	173	170	161	150	189

Data representative of DOE Contractor investigations

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

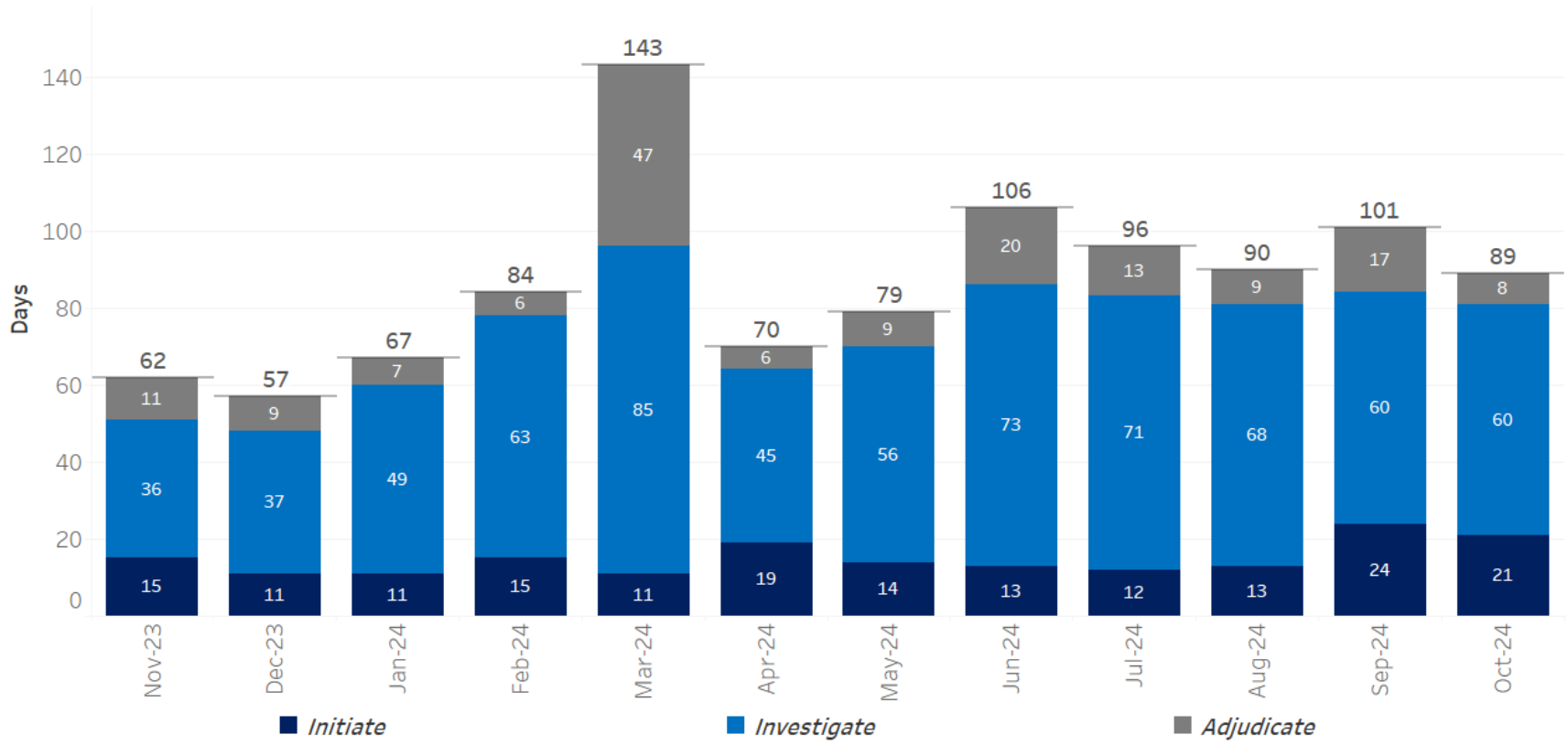


Number of Adjudications Reported

Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	Jul-24	Aug-24	Sep-24	Oct-24
96	79	79	74	98	89	109	114	131	97	76	106

Data representative of DOE Contractor investigations

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



Number of Adjudications Reported

Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	Jul-24	Aug-24	Sep-24	Oct-24
29	21	32	24	24	37	32	43	63	44	55	51

Data representative of DOE Contractor investigations

NRC
Chris Heilig

WORKLOAD & TIMELINESS PERFORMANCE METRICS

Nuclear Regulatory Commission

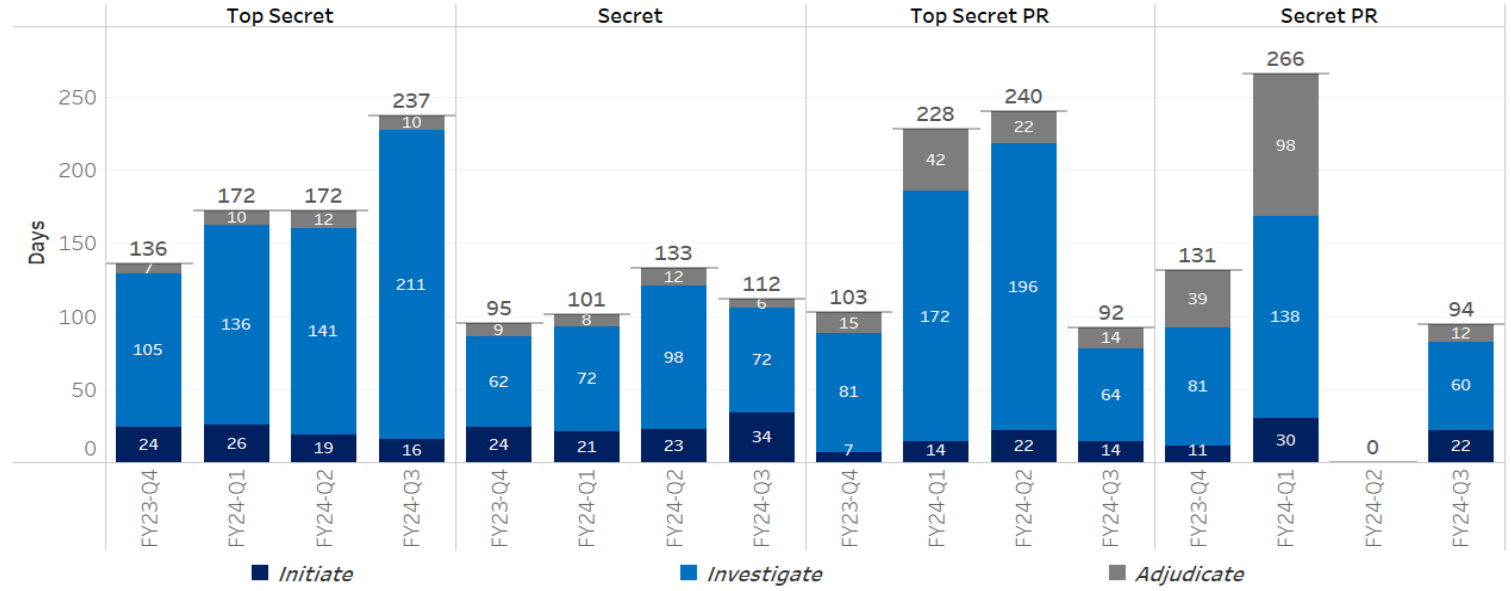
PERSONNEL SECURITY BRANCH
DIVISION OF FACILITIES AND SECURITY
OFFICE OF ADMINISTRATION
U.S. NUCLEAR REGULATORY COMMISSION

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Quarterly NRC Timeliness Performance Metrics

Average Days for Fastest 90% of Reported Clearance Decisions Made

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment



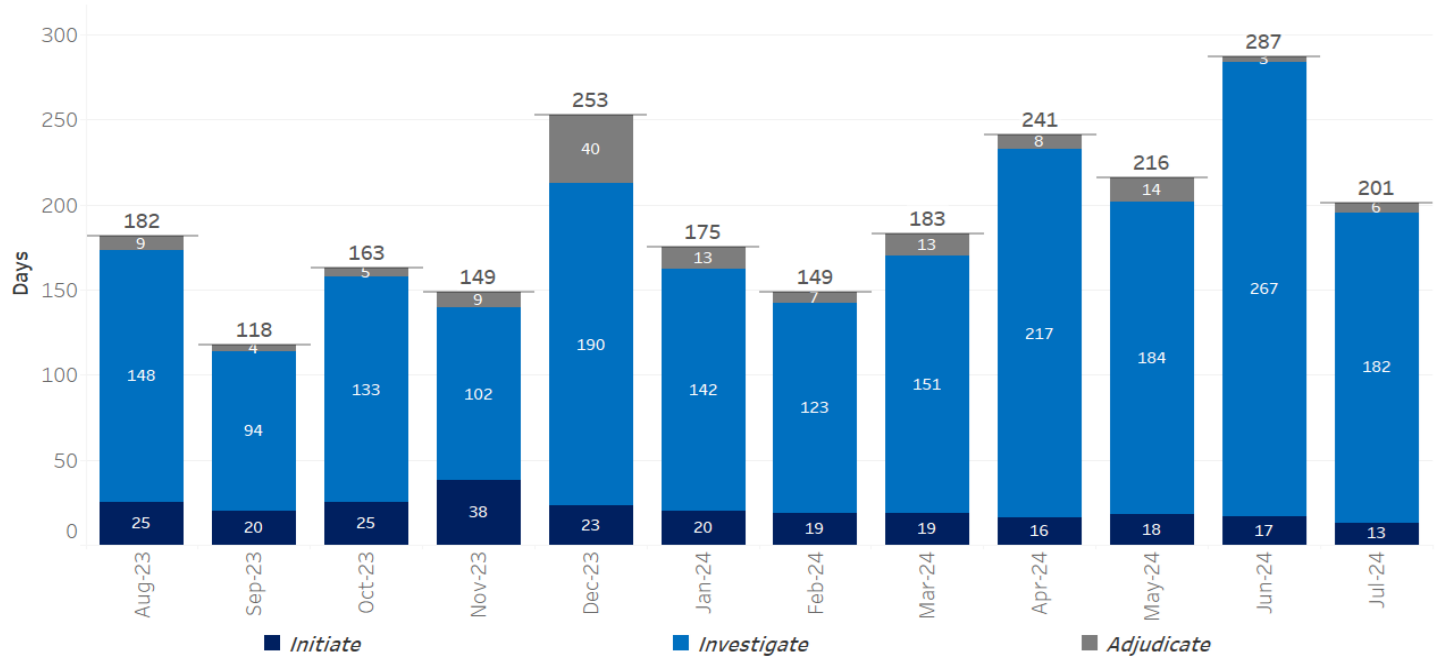
Total Adjudications Reported

	Top Secret	Secret	Top Secret PR	Secret PR
FY23-Q4	26	83	3	9
FY24-Q1	19	69	5	6
FY24-Q2	33	78	1	0
FY24-Q3	30	125	12	5

Quarterly NRC Timeliness Performance Metrics

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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

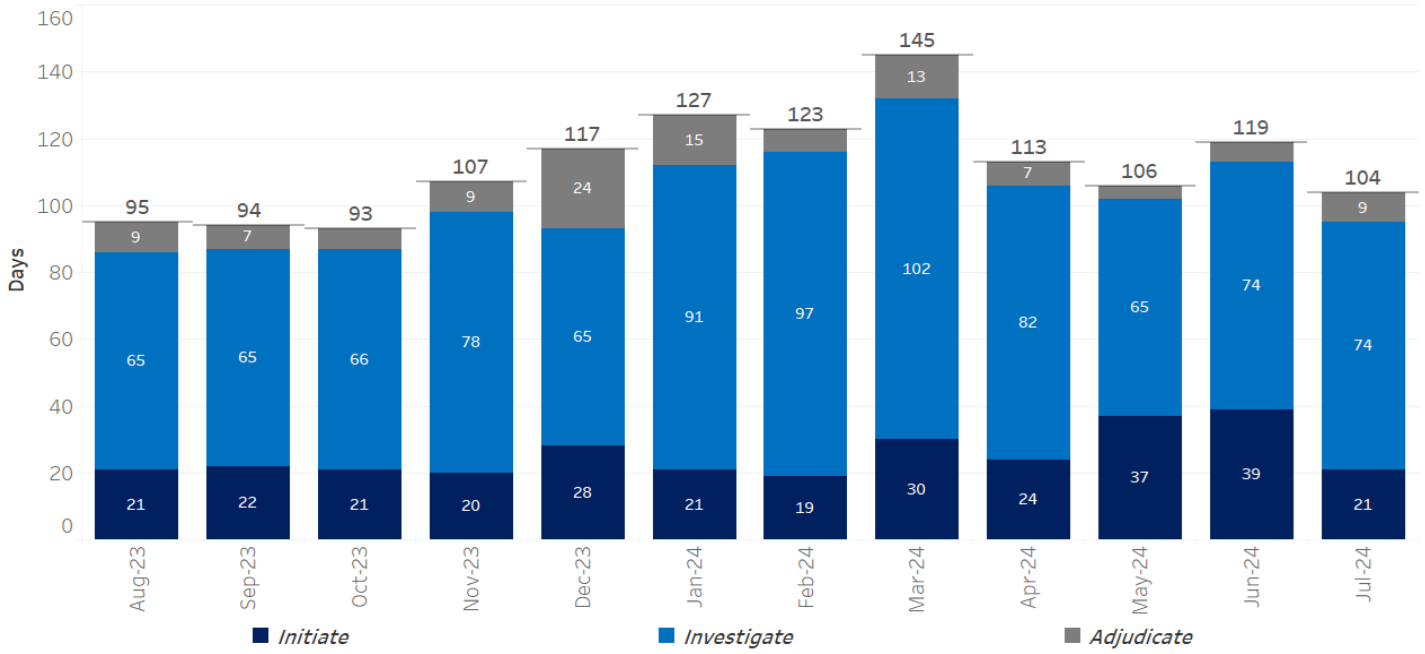


Number of Adjudications Reported

Aug-23	Sep-23	Oct-23	Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	Jul-24
8	9	10	3	6	13	8	12	10	14	6	7

Quarterly NRC Timeliness Performance Metrics

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

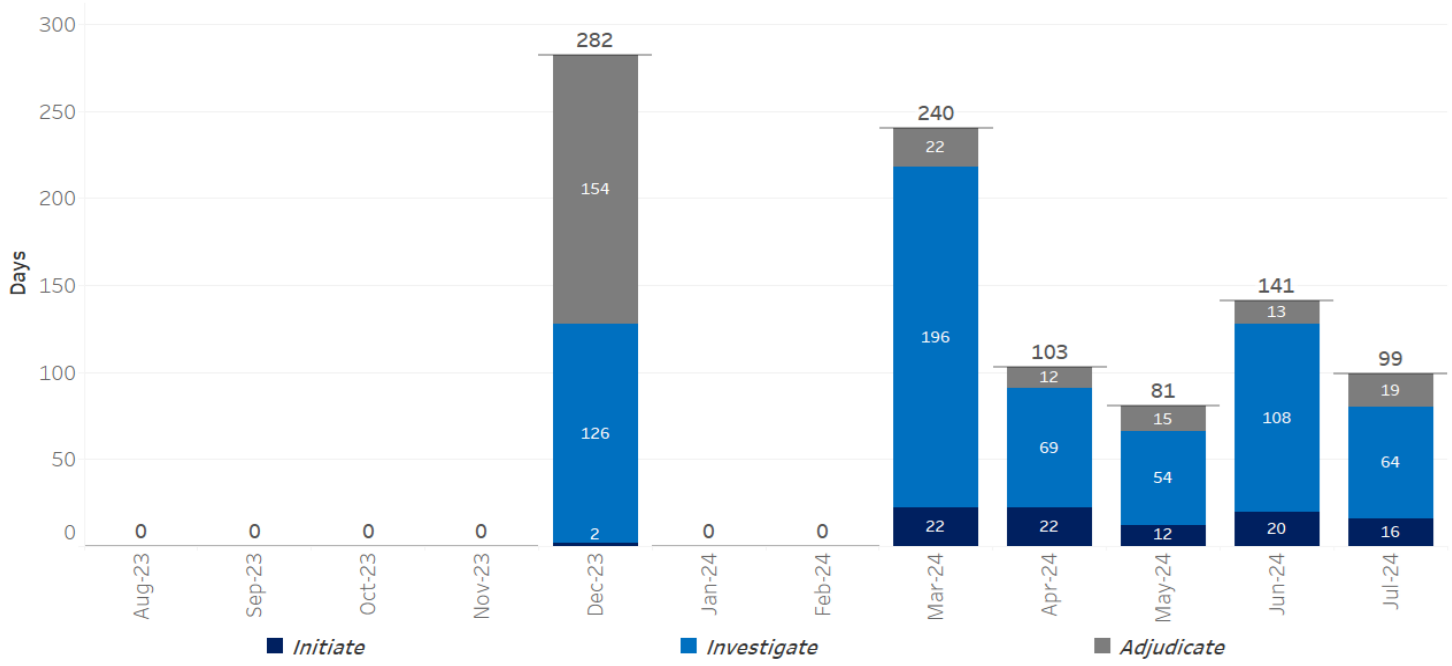


Number of Adjudications Reported

Aug-23	Sep-23	Oct-23	Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	Jul-24
34	19	29	22	19	23	26	27	35	46	44	43

Quarterly NRC Timeliness Performance Metrics

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



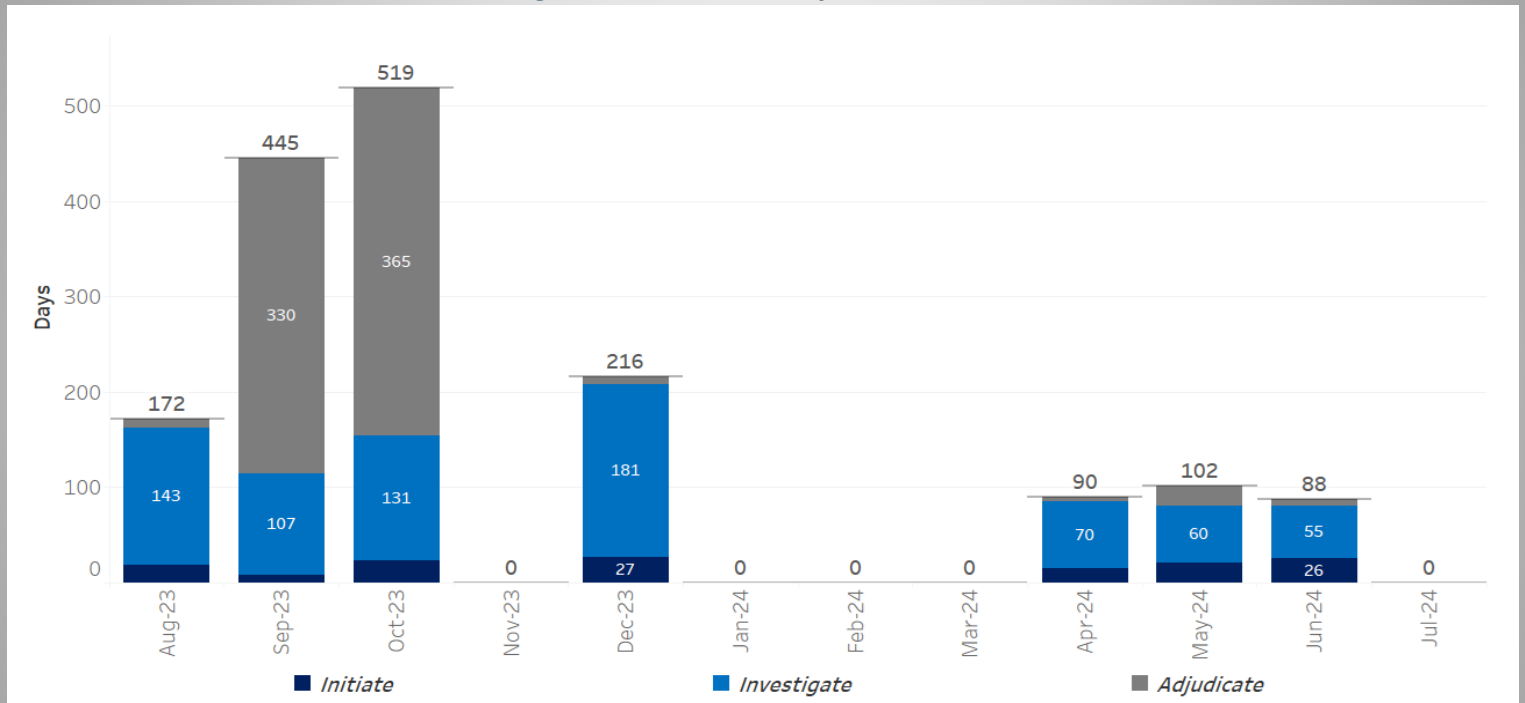
Number of Adjudications Reported

Aug-23	Sep-23	Oct-23	Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	Jul-24
0	0	0	0	1	0	0	1	2	7	2	2

Quarterly NRC Timeliness Performance Metrics

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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



Number of Adjudications Reported

Aug-23	Sep-23	Oct-23	Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	Jul-24
2	2	3	0	2	0	0	0	1	2	2	0

DCSA NCSO

Dave Scott

DCSA
NISA WG

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

DAVID SCOTT
NISP CYBERSECURITY OFFICE
INDUSTRIAL SECURITY DIRECTORATE

NISP eMASS Enhancements

- The Enterprise Mission Assurance Support Service (eMASS) is an application that is owned by the Defense Information Systems Agency (DISA). The National Industrial Security Program (NISP) instance is one of ~59 instances of eMASS.
- The NISP Cybersecurity Office (NCSO) works with DISA to deploy several enhancements for the NISP eMASS application that create efficiencies for all stakeholders, streamline the assessment and authorization process, and addresses concerns raised by Industry.
- The NCSO's goal is to continue to enhance eMASS functionality by further customizing the NISP instance, providing increased visibility, and improving metric capabilities to provide insight into timeliness & efficiencies.

FY24 Implemented NISP eMASS Enhancements

- NISP eMASS Release 5.11 and 5.11.1 deployed in March and June 2024.
- The highlights of the NISP enhancements included:
  - Improved system registration
  - Tailored system information fields to better support NISP processes
  - Updated NISP generated emails to remove CUI marking
  - User navigation tools that included information icons with Industry guidance
  - Customized auto-generated authorization letters (replacing authorization templates)
  - Enhanced metrics and reporting capability
  - Incorporated metadata within system artifacts bulk downloading
  - Added filters and fields within executive and system-level dashboards/reports
  - Improved User Interface/User Experience
  - Import/export mechanism for system inheritance providers
  - Additional workflow package actions
  - Continued improvement to existing modules

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.

NISP eMASS Resources

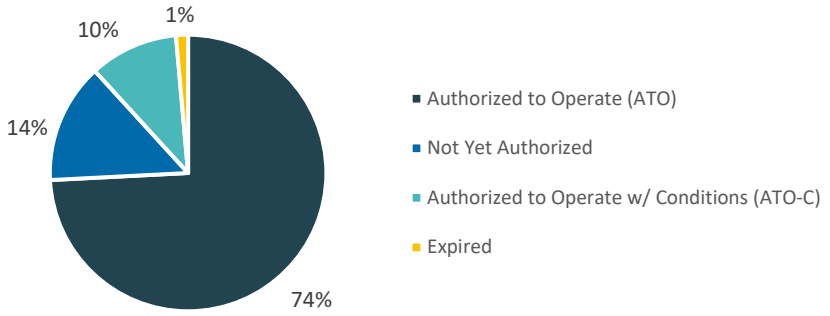
- NISP eMASS Release Notes, guides, templates, and job aids are available on the NISP eMASS HELP page: https://nisp.emass.apps.mil/App/Help/Home
- Monitor the NISP eMASS Announcements.
- Contact the DCSA NISP eMASS Team: dcsa.quantico.dcsa.mbx.emass@mail.mil

National-Level Metrics

NCSO Baseline Stats:

- The NISP Cybersecurity Office oversees ~5,200 classified IT systems as a part of the of National Industrial Security Program (NISP).
- The Industrial Security (IS) instance of eMASS had over 3,600 users and processed over 2100 authorizations by the end of FY24.
- ~35% of systems in the NISP have a Plan of Action & Milestone (POA&M) in process to address security controls and safeguarding efforts.

System Authorization Statuses Within the NISP



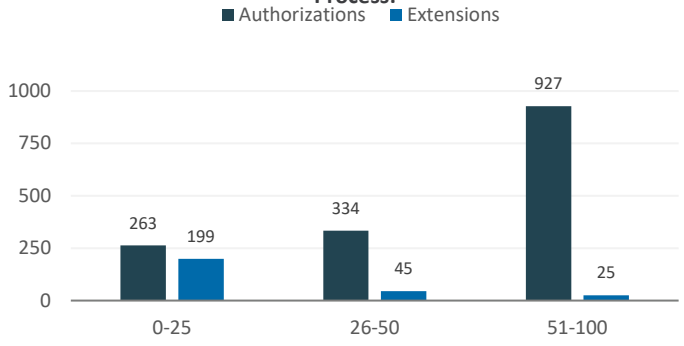
*Note: Denial of Authorization to Operate (DATO) & Interim Authorization to Test (IATT) omitted as combined total equals <1%

Median # of Days for NISP eMASS Authorization Decision:

IS Business Plan: < 90 Days

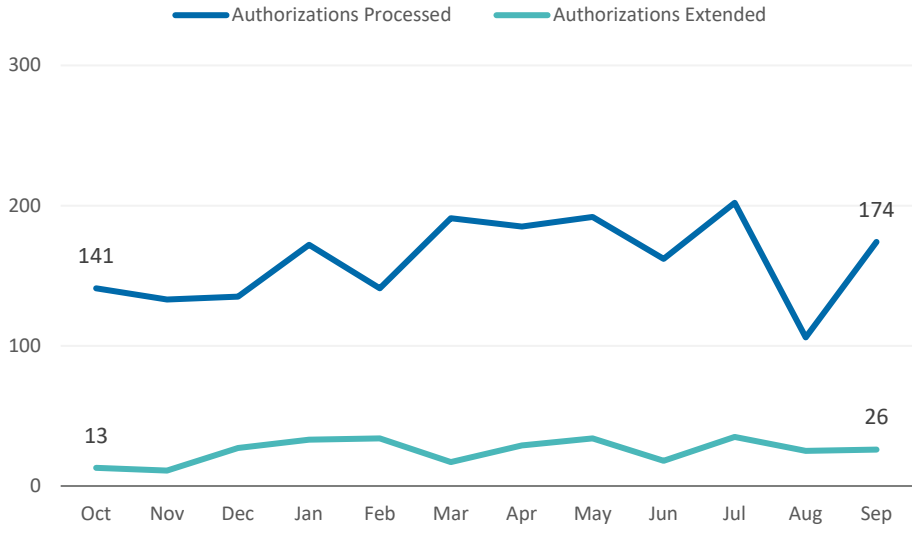
Med. Days for	Med. Days for Extensions:
75 Days	11 Days

Number of Completed Workflows by Days to Process:



Days for NISP eMASS Authorizations include both days in industry and days with DCSA

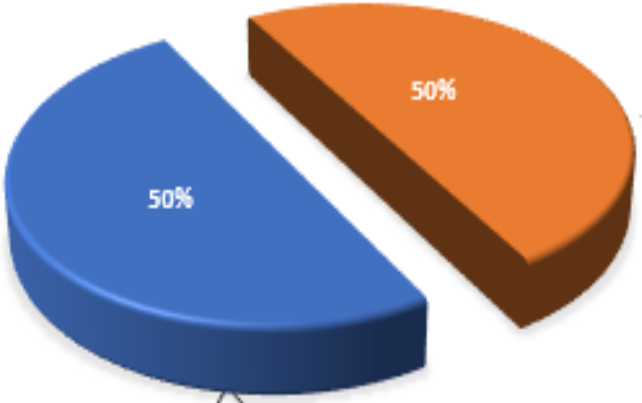
Number of Authorizations Processed and Extended



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

CORA Components



Orders / Directives/ Policies – 50%

- Endpoint Security – Weight 4
- Network Vulnerability Scan – Weight 4
- Insider Threat (NSS Only) – Weight 2
- Cross Domain Solution – Weight 5
- Cyber Defense Monitoring, Detection, Response – Weight 5
- Cybersecurity and Resiliency – Weight 2
- SCRM (multiple policies) – Weight 1

Cyber Maintenance – 50%

- Boundary (Defined in notes) - Weight 5
- CDS (combined) - Weight 5
- Network Vulnerability Scan - Weight 4
- Endpoint Security (If STIGs exist) - Weight 4
- Internal Network - Weight 4
- Domain Name System (DNS) – Weight 3
- Traditional Security – Weight 3
- Mobility – Weight 3
- Internal Web Server – Weight 2
- Internal Database - Weight 2
- Releasable Networks (REL) Weight 2
- Exchange – Weight 2
- Video/Voice Over IP (VVOIP) – Weight 2
- Virtual Infrastructure –Weight 2
- Windows/UNIX OS – Weight 1
- Other – Weight 1

Overrides

- Boundary vulnerabilities tied to KIOR result in a Severity Override of two levels
  - Example: Moderate Risk → High Risk → **Very High Risk**
- Internal vulnerabilities linked to KIOR result in a Severity Override of one level
  - Example: Moderate Risk → **High Risk**
- Measure indicators linked to KIOR will result in Critical Override that makes the measure receive a "zero" score
- Mitigation demonstrated up channel may negate a Severity Override pending Team Lead determination
- KIOR can be remediated

Key Indicators of Risk

Control Access

- Deny by Default Posture
- 802.1x / C2C
- Encryption
- Permissions Management

Minimum Defensive Posture

- Highly Exploitable Vulnerabilities (J2 / ACAS)
- Account Management
- End of Life / End of Support

Detect Anomalies

- Monitor Network Traffic
- Endpoint Security
- CSSP
- Privileged Shell Management
- Network Vulnerability Scan
- Log Review / Monitoring

Mission Assurance

- MRT-C / MADSS
- COOP / Disaster Recovery

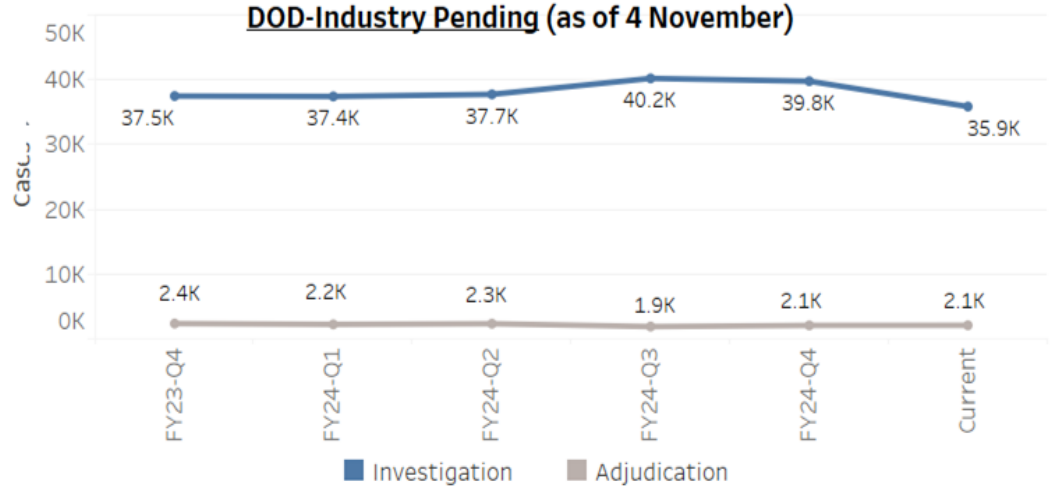
KIORs tie directly to CORA scoring through severity and critical overrides impacting scoring and reinforcing JFHQ-DODIN cybersecurity priorities

DCSA AVS
Various Speakers

DCSA INVENTORY & TIMELINESS | *Industry*

INVENTORY (includes only T5/T3/T5R/T3R)

DOD-Industry Pending (as of 4 November)



DoD-Industry Pending by Case Type (as of 4 November)

Investigation Inventory

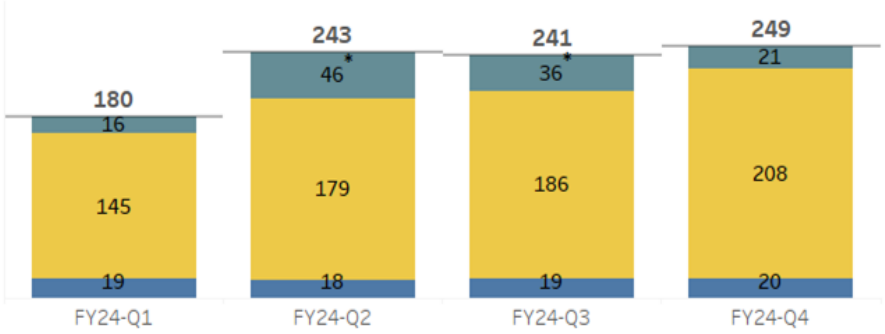
T5			T3		
FY24 Start	FY24 End	Current	FY24 Start	FY24 End	Current
18.5K	21.1K	19.6K	18.3K	18.5K	16.2K

Adjudication Inventory

T5			T3		
FY24 Start	FY24 End	Current	FY24 Start	FY24 End	Current
418	523	575	1.5K	1.1K	1.1K

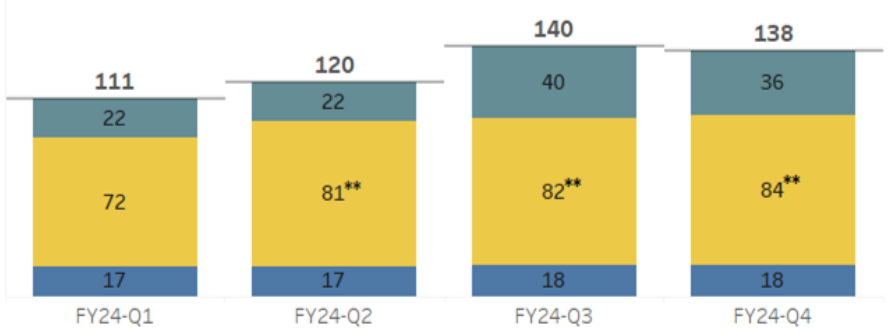
END-TO-END TIMELINESS (Fastest 90% of Adjudicated Cases)

INITIAL TOP SECRET - DOD INDUSTRY



*DISS technical issue impacting ~900 Top Secret adjudications in Q2 and ~440 in Q3 resulted in a temporary spike in timeliness. Adjudication timeliness for unaffected cases averaged 20 days during Q2 and 31 days during Q3.

INITIAL SECRET - DOD INDUSTRY



**Delays in FBI Name Checks negatively impacted investigation timeliness for Secret cases. 1.1K Secret investigations in Q2 and 1.3K in Q3 were completed where receipt of the FBI Name Check was the last pending item for completion. Timeliness for the unaffected cases was 78 days in Q2 & 79 days in Q3 & Q4.

Initiate | Investigate | Adjudicate

DOHA Update

Perry Russell-Hunter

(no slides)

General Discussion

Closing Remarks
ISOO

Back Up Slides
(Working Group Updates)

NISPPAC Working Groups

- NISP Information Systems Authorization (NISA)
  - Various items
  - Last mtg 10/30/2024
- Clearance
  - Various items
  - Last mtg 9/4/2024
- Cost
  - Cognizant Security Agencies/Offices only at this time
  - Discussed how to collect costs of NISP for Industry
  - Last mtg 11/30/2022
- Policy
  - Status of various Industrial Security policies
  - Last mtg 9/7/2022

NISPPAC Working Groups

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

- NISP Systems
  - Discussed the systems associated with the NISP program at the various CSAs
  - Last mtg 9/10/2020

NISPPAC Working Groups

- Insider Threat
  - Discussed training and certification of security professionals, insider threat plans, Section 9403 of the NDAA for FY 2021 (federal policy on the sharing of information pertaining to contractor employees in the trusted workforce)
  - Last mtg 9/2/2020