INDUSTRIAL SECURITY

CHANGES AND ADAPTATIONS

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Matthew Redding, Assistant Director

AGENDA

PURPOSE

To provide an overview of the changing operational environment and adaptations DCSA is making in response

OUTCOMES

Increase awareness and understanding about DCSA, Industrial Security, and the current operational environment

AGENDA

⇨ DCSA and Industrial Security Overview

⇨ Operational Environment

⇨ Changes and Adaptations

⇨ Closeout

⇨ Q&A

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY | 2

DCSA INTRODUCTORY VIDEO

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

DCSA AND INDUSTRIAL SECURITY OVERVIEW

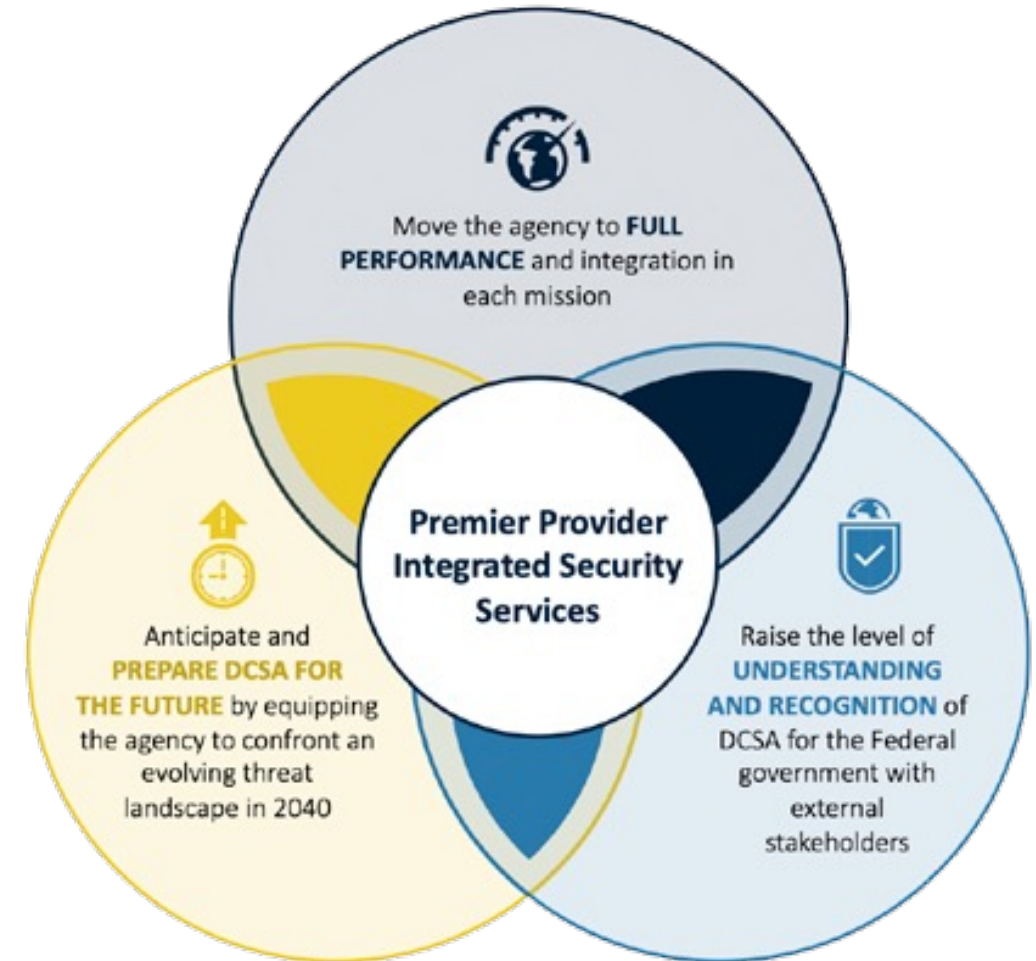**DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY**

DCSA STRATEGIC PRIORITIES

As the nation's premier provider of integrated security services, DCSA is committed to steadfast excellence in the execution of our national security mission and unwavering commitment to efficiency as model stewards of taxpayer funds. We align to and support Presidential and Defense priorities.

In 2025, DCSA publicly released an updated strategy focused on three strategic priorities.

PRESIDENTIAL AND DEFENSE PRIORITIES

- Restoring trust through efficient and effective stewardship of taxpayer dollars
- Achieving strength through direct support to the Defense Industrial Base
- Reestablishing deterrence through lethality, meritocracy, accountability, standards and readiness

Move the agency to **FULL PERFORMANCE** and integration in each mission

Premier Provider Integrated Security Services

Anticipate and **PREPARE DCSA FOR THE FUTURE** by equipping the agency to confront an evolving threat landscape in 2040

Raise the level of **UNDERSTANDING AND RECOGNITION** of DCSA for the Federal government with external stakeholders

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

DCSA MISSION, VISION AND VALUES

MISSION:

Through vetting, industry engagement, education, and counterintelligence and insider threat support, secure the trustworthiness of the United States Government's workforce, the integrity of its cleared contractor support, and the uncompromised nature of its technologies, services, and supply chains.

VISION:

DCSA is America's Gatekeeper: safeguarding the Nation as the **premier provider of integrated security services** – national security is our mission; people are our greatest asset.

VALUES:

- Committed to Mission
- Invested in People
- Passionate about Service
- Unwavering in Integrity
- Driven to Innovate

LARGEST INTEGRATED SECURITY AGENCY: WE ARE IN THE TRUST BUSINESS

Personnel Security (PS): Vetting and establishing trust in America's federal and contractor workforce

Industrial Security (IS): Partnering with Industry to maintain trust in America's workspace and classified technologies

Counterintelligence and Insider Threat (CI): Preserves America's foundation of trust against foreign and insider threats

Security Training (ST): Training and empowering security professionals to build a trustworthy workforce

Field Operations (FO): Enabling trust through mission support and information sharing in the field

DCSA IS A SECURITY SERVICE PROVIDER FOR DoD AND FEDERAL GOVERNMENT — WE OPERATE LIKE A BUSINESS

Manages the NISP for DoD and **35** Federal Agencies	**$3.085 B** DCSA FY25 Budget	WCF - $2.055 B App. - $1.030B	**174** Field Locations
10 K/13 K Cleared Companies / FCLs	**2.7+ M** Annual Investigations	**10.7 K** Per Day	**4** Consolidated Regions

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

OPERATIONAL ENVIRONMENT

**DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY**

FRAMING THE THREAT

REPORTING

■	East Asia & the Pacific	37%
■	Near East	25%
■	Europe & Eurasia	17%
■	South & Central Asia	10%
■	Western Hemisphere	6%
■	Africa	1%
□	Unknown	4%

TOP METHODS OF OPERATION

- Résumé Submission
- Exploitation of Business Activities
- Exploitation of Experts
- Request for Information/Solicitation
- Exploitation of Cyber Operations

TOP TARGETED TECHNOLOGIES

- Electronics
- Software
- Command, Controls, Communication, & Computers (C4)
- Aeronautic Systems
- Services and Other Products
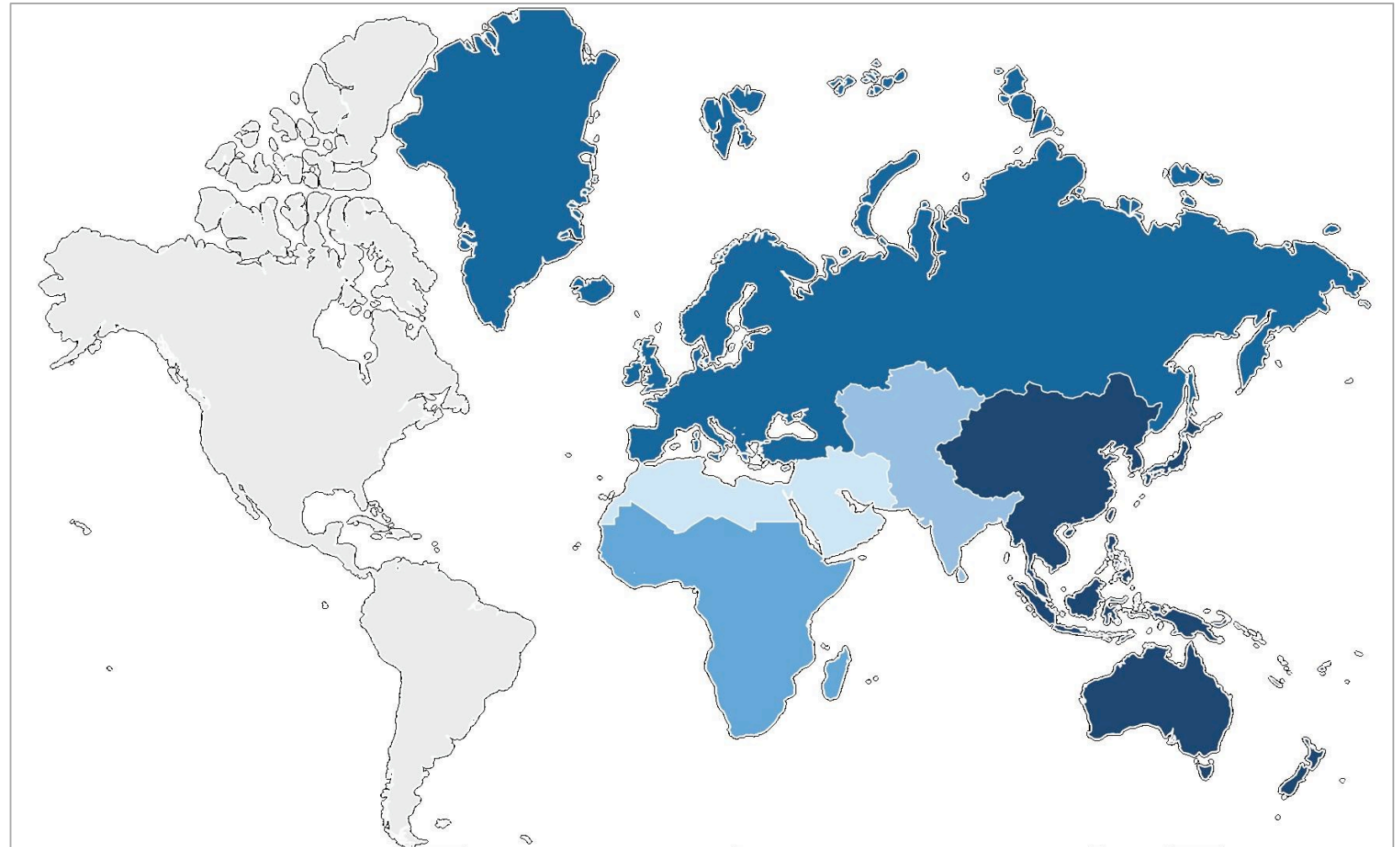
DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

CHINA THREAT SNAPSHOT

BETWEEN JAN. 2021 - FEB. 2025 THERE HAVE BEEN

60+ CCP-RELATED ESPIONAGE CASES ACROSS **20** STATES

THOSE CASES INCLUDE:

- **TRANSMISSION** OF SENSITIVE MILITARY INFORMATION TO THE PRC

- **STEALING** OF TRADE SECRETS TO BENEFIT THE PRC

- **TRANSNATIONAL** REPRESSION SCHEMES TO TARGET PRC DISSIDENTS

- **OBSTRUCTION** OF JUSTICE

- **ROUGHLY** EVERY 12 HOURS THE FBI OPENS A NEW CASE TO COUNTER THE PRC'S INTELLIGENCE OPERATIONS

SOURCE: HOMELAND.HOUSE.GOV

RAPID EXPANSION OF CCP-RELATED ESPIONAGE AND ACTS OF TRANSNATIONAL REPRESSION THROUGHOUT THE US:

DARKER COLORS INDICATE STATES WITH MORE CCP-RELATED ESPIONAGE CASES

"Today, the Chinese Communist Party poses a military threat to America and our allies, an economic threat to our companies, and an ideological challenge around the world."
- Chairman Rep. John Moolenar of the House Select Committee on the CCP, Jan. 22, 2025.

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

CHINA THREAT SNAPSHOT
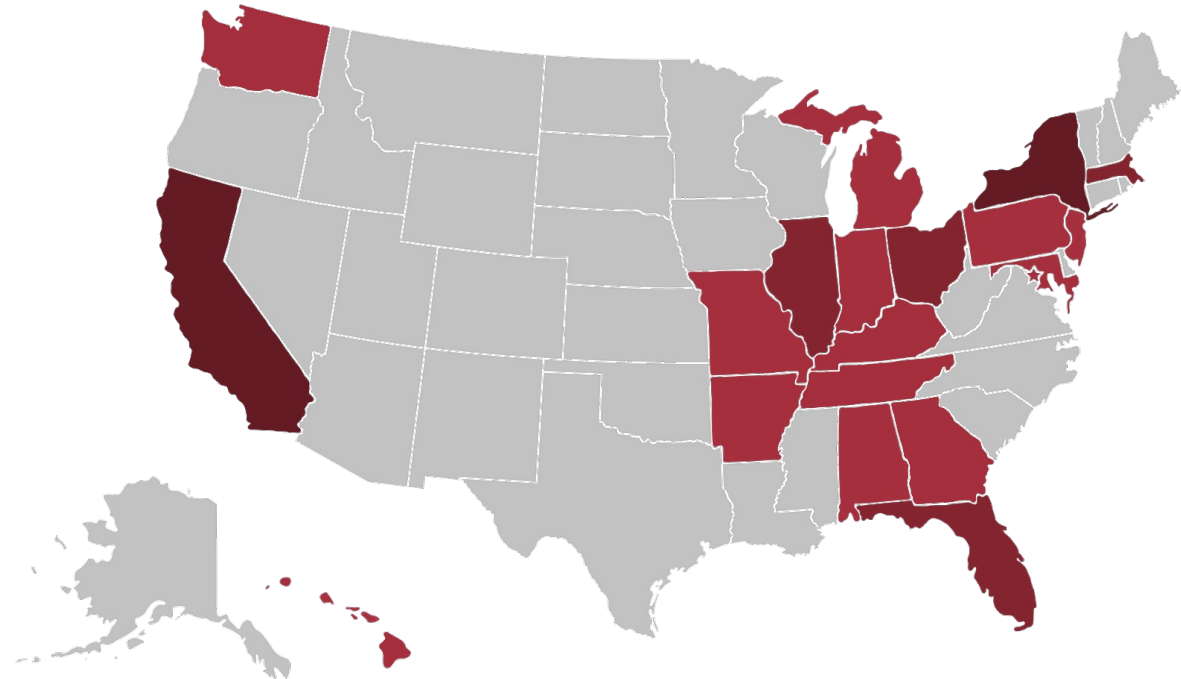
BETWEEN JAN. 2021 - FEB. 2025 THERE HAVE BEEN

60+ CCP-RELATED ESPIONAGE CASES ACROSS **20** STATES
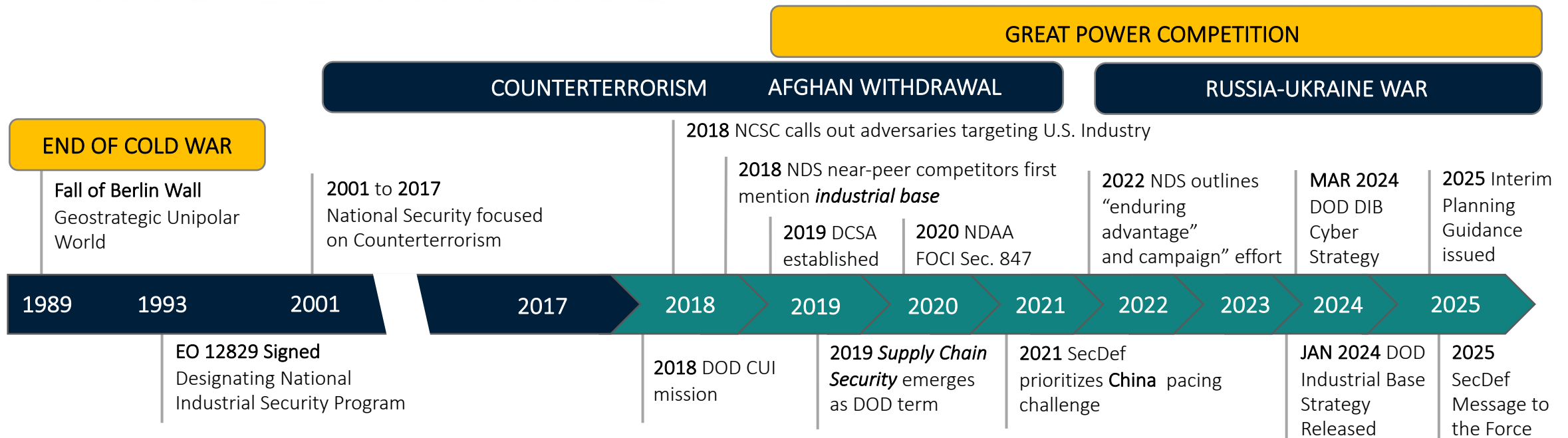
THOSE CASES INCLUDE:

- **TRANSMISSION** OF SENSITIVE MILITARY INFORMATION TO THE PRC

- **STEALING** OF TRADE SECRETS TO BENEFIT THE PRC

- **TRANSNATIONAL** REPRESSION SCHEMES TO TARGET PRC DISSIDENTS

- **OBSTRUCTION** OF JUSTICE

- **ROUGHLY** EVERY 12 HOURS THE FBI OPENS A NEW CASE TO COUNTER THE PRC'S INTELLIGENCE OPERATIONS

SOURCE: HOMELAND.HOUSE.GOV
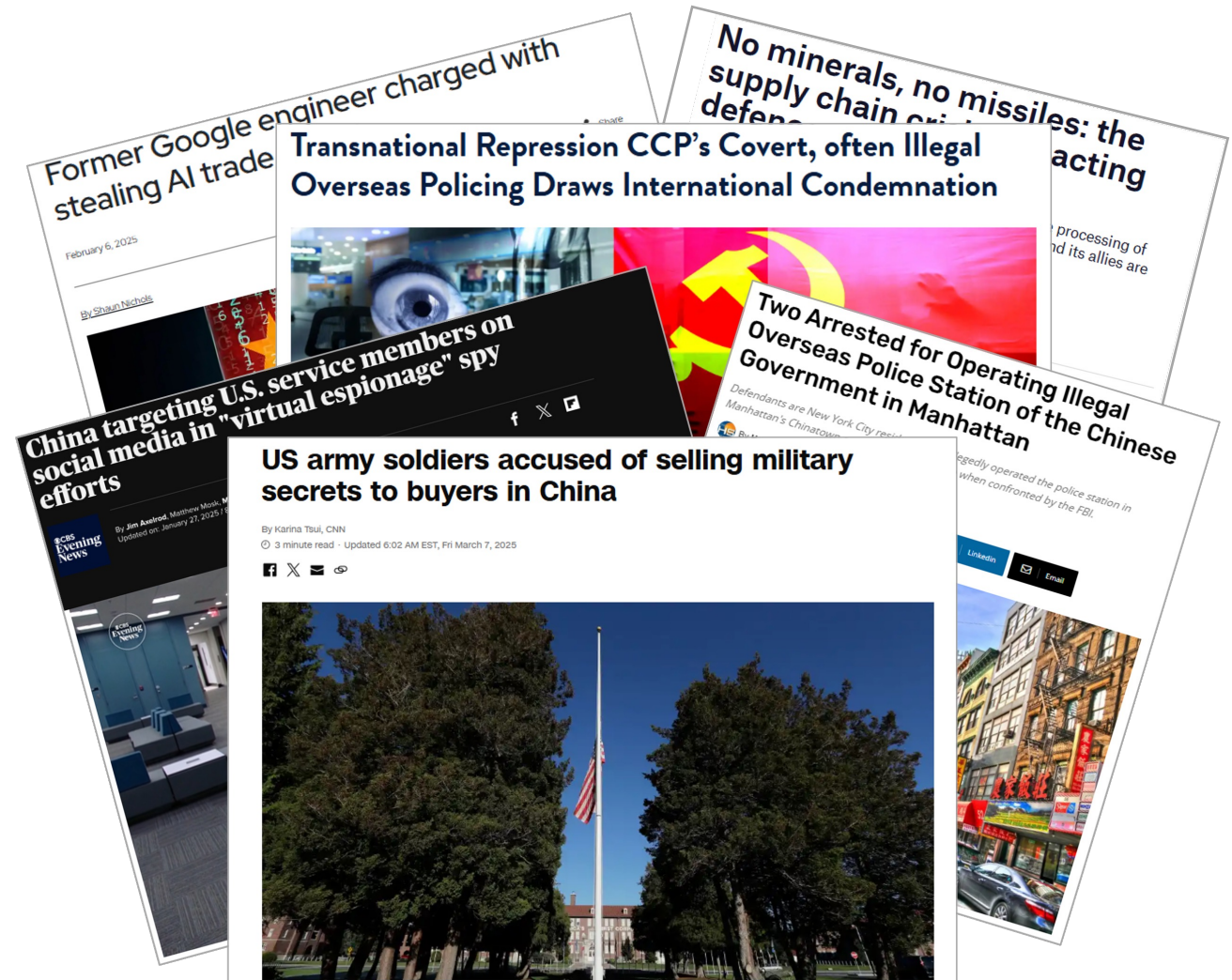
SHIFTING STRATEGIC ENVIRONMENT

GREAT POWER COMPETITION

COUNTERTERRORISM **AFGHAN WITHDRAWAL** **RUSSIA-UKRAINE WAR**

2018 NCSC calls out adversaries targeting U.S. Industry

END OF COLD WAR

2018 NDS near-peer competitors first mention *industrial base*

Fall of Berlin Wall
Geostrategic Unipolar World

2001 to **2017**
National Security focused on Counterterrorism

2022 NDS outlines "enduring advantage" and campaign" effort

MAR 2024 DOD DIB Cyber Strategy

2025 Interim Planning Guidance issued

2019 DCSA established

2020 NDAA FOCI Sec. 847

1989	1993	2001	2017	2018	2019	2020	2021	2022	2023	2024	2025

EO 12829 Signed
Designating National Industrial Security Program

2018 DOD CUI mission

2019 *Supply Chain Security* emerges as DOD term

2021 SecDef prioritizes **China** pacing challenge

JAN 2024 DOD Industrial Base Strategy Released

2025 SecDef Message to the Force

RELEASE
IMMEDIATE RELEASE

Secretary Hegseth's Message to the Force

Jan. 25, 2025 | f X ↱

"We will rebuild our military by matching threats to capabilities. This means reviving our defense industrial base, reforming our acquisition process, passing a financial audit, and rapidly fielding emerging technologies. We will remain the strongest and most lethal force in the world…"
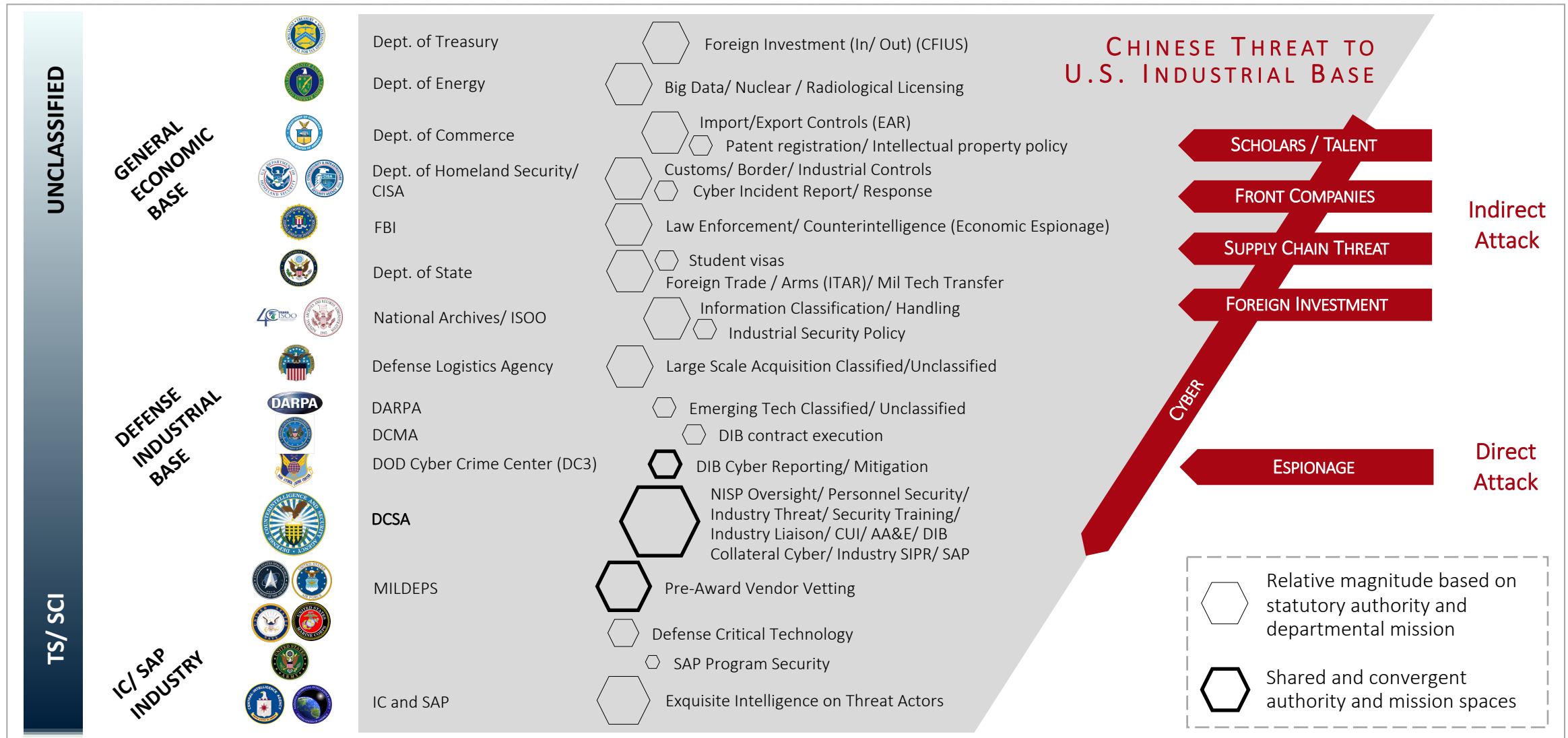
Chinese theft of U.S. intellectual property is estimated at $225B to $600B annually.
Source: FBI estimate 2020

How China plans to surpass the U.S. as a manufacturing and military power:
• Conducting fraud, espionage, and other illicit practices
• Exploiting free-market systems
• Targeting technologies essential for maintaining U.S. national security advantage

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

INDUSTRIAL SECURITY CENTER OF GRAVITY

UNCLASSIFIED

TS/SCI

GENERAL ECONOMIC BASE

Agency	Mission
Dept. of Treasury	Foreign Investment (In/ Out) (CFIUS)
Dept. of Energy	Big Data/ Nuclear / Radiological Licensing
Dept. of Commerce	Import/Export Controls (EAR) / Patent registration/ Intellectual property policy
Dept. of Homeland Security/ CISA	Customs/ Border/ Industrial Controls / Cyber Incident Report/ Response
FBI	Law Enforcement/ Counterintelligence (Economic Espionage)
Dept. of State	Student visas / Foreign Trade / Arms (ITAR)/ Mil Tech Transfer
National Archives/ ISOO	Information Classification/ Handling / Industrial Security Policy

DEFENSE INDUSTRIAL BASE

Agency	Mission
Defense Logistics Agency	Large Scale Acquisition Classified/Unclassified
DARPA	Emerging Tech Classified/ Unclassified
DCMA	DIB contract execution
DOD Cyber Crime Center (DC3)	DIB Cyber Reporting/ Mitigation
DCSA	NISP Oversight/ Personnel Security/ Industry Threat/ Security Training/ Industry Liaison/ CUI/ AA&E/ DIB Collateral Cyber/ Industry SIPR/ SAP
MILDEPS	Pre-Award Vendor Vetting

IC/ SAP INDUSTRY

Agency	Mission
	Defense Critical Technology
	SAP Program Security
IC and SAP	Exquisite Intelligence on Threat Actors

CHINESE THREAT TO U.S. INDUSTRIAL BASE

- SCHOLARS / TALENT
- FRONT COMPANIES
- SUPPLY CHAIN THREAT
- FOREIGN INVESTMENT

Indirect Attack

CYBER

- ESPIONAGE

Direct Attack

Relative magnitude based on statutory authority and departmental mission

Shared and convergent authority and mission spaces

CHANGES AND ADAPTATIONS

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

PUBLIC LAW 116-92, SECTION 847

CHANGE: SECURITY FOR THE DEFENSE INDUSTRIAL BASE

ADAPTATION: EXPANDING DCSA AUTHORITIES

> Section 847 of Public Law 116-92 requires the DoD to improve its risk assessment and mitigation of foreign ownership, control, or influence (FOCI) of its contractors and subcontractors.

1 Reinforced by DoD Instruction 5205.87: Mitigating Risks related to FOCI for Contractors and Subcontractors

2 Applies to *all* contracts > $5M, including those that are unclassified, and grants DCSA oversight throughout the pre-contract award phase

3 Provides better insight into potential risks associated with FOCI

Annual 847 New Case Processing Workload				Cumulative Annual Oversight
41,000 case reviews	17,600 FOCI assessments*	13,500 risk management strategies	7,500 implemented risk management strategies	9,000 formal oversight actions

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

FACILITY CLEARANCE PROCESS

CHANGE: FCL PROCESS IS STABLE

ADAPTATION: IMPROVING PROCESS AND SERVICE OUTPUT

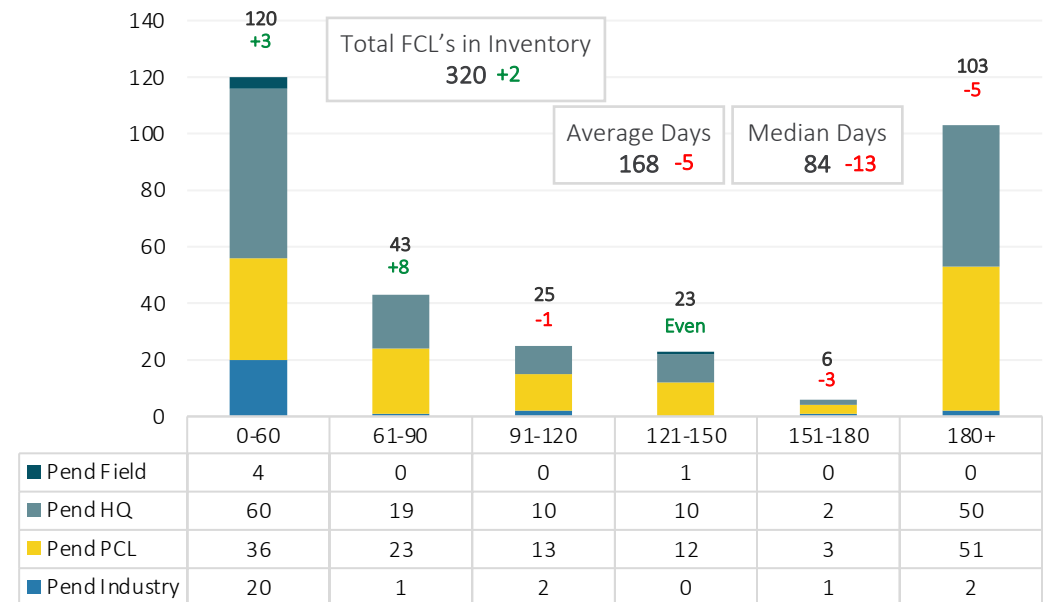| Tier	Plan	Actual	Quickest 80%
Sponsorship	15	9	N/A
Tier 1	60	48	34
Tier 2	90	0	0
Tier 3	180	273	228

1 The FY 25 Initial and Upgrade FCL packages inventory goal is < or = 300.

2 DCSA continues to examine metrics and processes to make additional improvements, as appropriate.

INITIAL/UPGRADE FCL PACKAGE INVENTORY

Total FCL's in Inventory
320 +2

Average Days
168 -5

Median Days
84 -13

	0-60	61-90	91-120	121-150	151-180	180+
Pend Field	4	0	0	1	0	0
Pend HQ	60	19	10	10	2	50
Pend PCL	36	23	13	12	3	51
Pend Industry	20	1	2	0	1	2

Column totals/labels: 120 +3, 43 +8, 25 -1, 23 Even, 6 -3, 103 -5

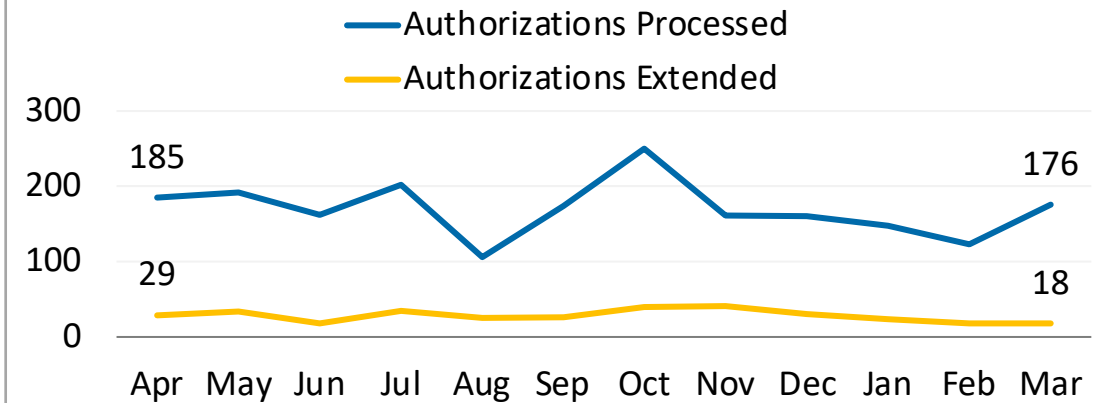**DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY**

15

NISP CYBERSECURITY

CHANGE: NUMBER OF SYSTEMS

ADAPTATION: ENHANCING eMASS AND WORKING WITH NISPPAC

SYSTEM AUTHORIZATION WITHIN THE NISP

- 2%
- 12%
- 14%
- 74%

- ■ Authorized to Operate (ATO)
- ■ Not Yet Authorized
- ■ Authorized to Operate w/ Conditions (ATO-C)
- ■ Expired
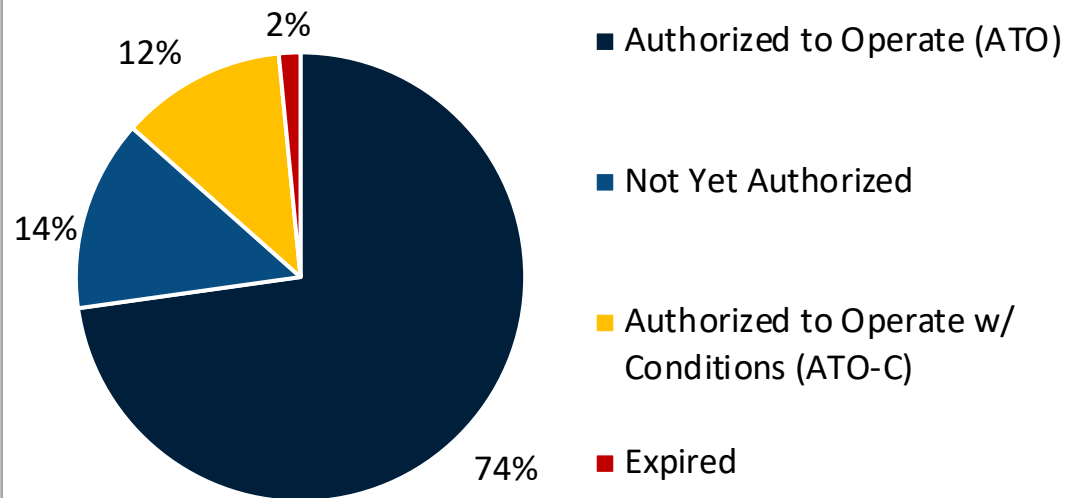
NUMBER OF AUTHORIZATIONS PROCESSED AND EXTENDED

— Authorizations Processed
— Authorizations Extended

185 ... 176
29 ... 18

Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar

AVERAGE # OF DAYS FOR NISP EMASS AUTHORIZATION

Days to Process Workflows

IS Business Plan (< 90 Days)

■ Authorizations ■ Extensions

0-25	26-50	51-100
244 / 225	320 / 41	969 / 27

Avg. Days for Authorizations
80 Days

Avg. Days for Extensions
28 Days

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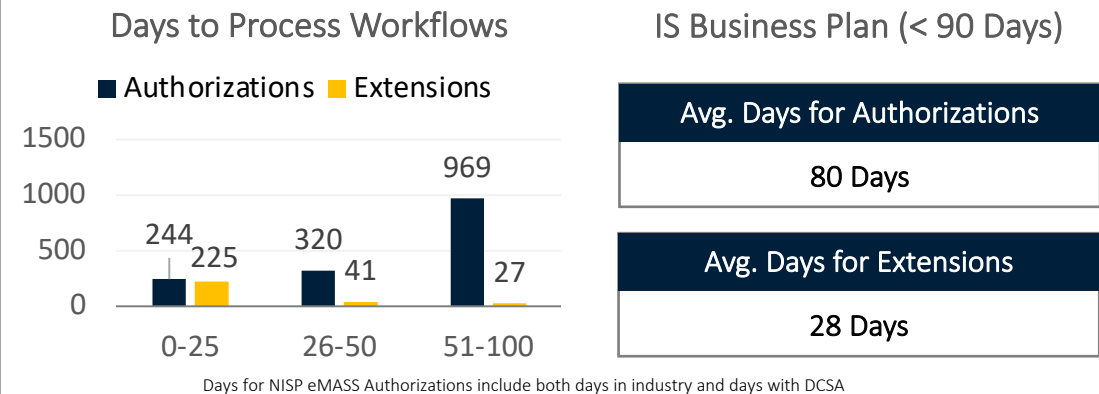
SECURITY REVIEW

CHANGE: SECURITY REVIEW SCORING

ADAPTATION: IMPLEMENTING THE INDUSTRIAL SECURITY SCORECARD

On October 1, 2024, DCSA implemented a Security Rating Scorecard, developed in partnership with NISPPAC Industry, which addresses requests for clarity and consistency – feedback has been positive.

FY 24 Total: 4,668
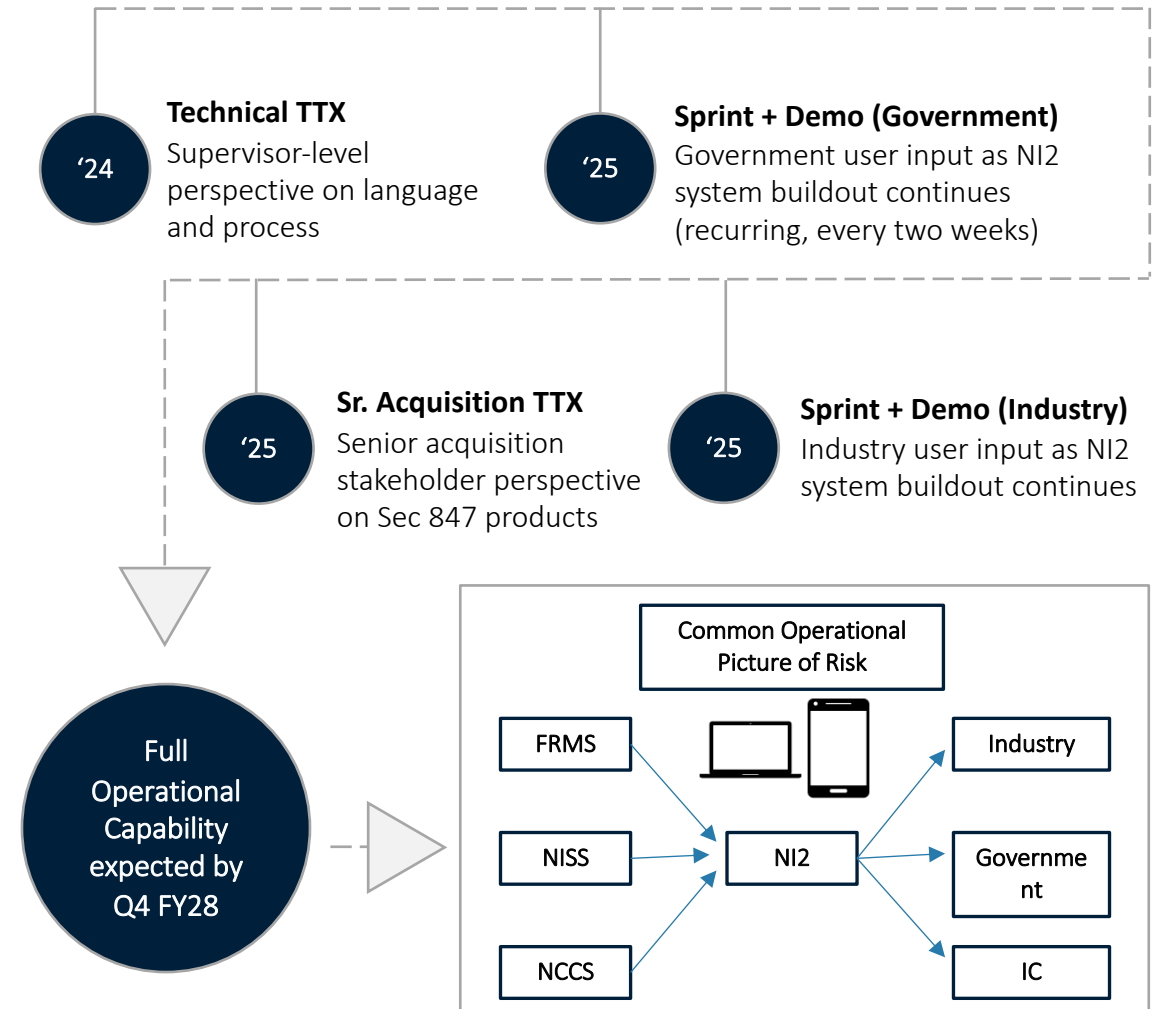**FY 25 Total:** 1,884

RATING PERCENTAGE COMPARISON CHART

	Superior	Commendable	Satisfactory	Marginal	Unsatisfactory
■ FY24 Average	6.2%	18.1%	74.8%	0.5%	0.5%
■ FY25 (Oct 1 - Mar 13)	14.0%	37.4%	47.5%	0.6%	0.5%

Bar values: Superior 287 / 262; Commendable 840 / 683; Satisfactory 3,466 / 891; Marginal 21 / 12; Unsatisfactory 21 / 11
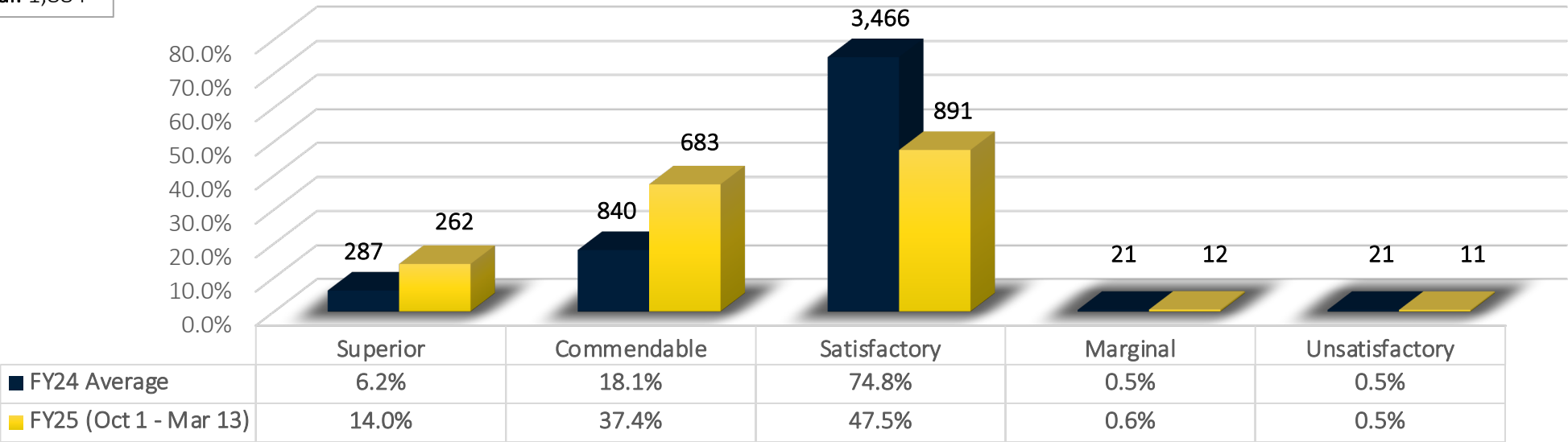
NATIONAL INDUSTRIAL SECURITY SYSTEM INCREMENT II

CHANGE: NI2 DEVELOPMENT

ADAPTATION: GREATER FOCUS ON SECTION 847

1 NI2 will incorporate workflows and functions required to support the National Industrial Security Program Contract Classification System bridge solution and Section 847.

2 The end products will provide a secure and resilient data ecosystem that delivers scalability of functionality to support industrial security.

'24 — Technical TTX Supervisor-level perspective on language and process

'25 — Sprint + Demo (Government) Government user input as NI2 system buildout continues (recurring, every two weeks)

'25 — Sr. Acquisition TTX Senior acquisition stakeholder perspective on Sec 847 products

'25 — Sprint + Demo (Industry) Industry user input as NI2 system buildout continues

Full Operational Capability expected by Q4 FY28

Common Operational Picture of Risk

FRMS

NISS

NCCS

NI2

Industry

Government

IC

INDUSTRIAL SECURITY POLICY

CHANGE: POLICY ENVIRONMENT

ADAPTATION: MORE DELIBERATE REVIEW OF POLICIES

1 **Industrial Security Letters**: Updated Insider Threat + DCSA Accreditation and Assessment Guide on hold (policy freeze)

2 **Defense Policies:** Volume 1 of DoD Manual 5220.32 – NISP Procedures for Government Activities

3 **Defense Federal Acquisition Regulation Supplement:** Possible delay (policy freeze)
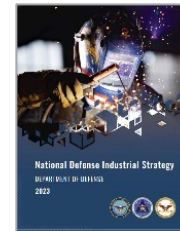
National

1. Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA)
2. Public Law 116-92, Section 847 Mission
3. CHIPS and Science Act of 2022
4. EO 14105: U.S. Investments in Certain National Security Technologies, Products in Countries of Concern
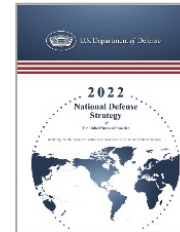
National Defense Strategy

1. Defend the homeland
2. Deter strategic attacks against U.S., Allies, and partners
3. Deter aggression and be prepared to prevail in conflict
4. Build a resilient Joint Force and defense ecosystem

National Defense Industrial Strategy

1. Resilient Supply Chains
2. Workforce Readiness
3. Flexible Acquisition
4. Economic Deterrence

Defense Industrial Base Cybersecurity Strategy

1. Strengthen DOD governance for DIB cybersecurity
2. Enhance cybersecurity posture of DIB
3. DIB capabilities' resiliency in cyber-contested environment
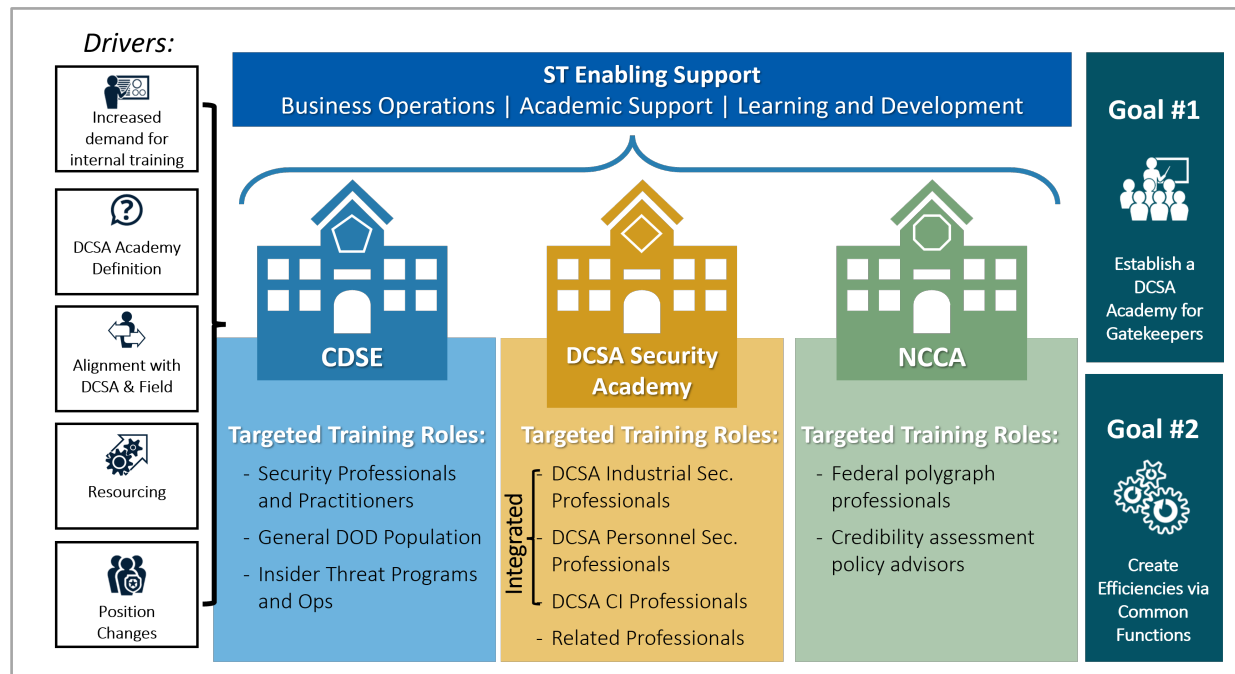4. Improve cybersecurity collaboration with DIB

SECURITY TRAINING

CHANGE: DCSA SERVICE PROVIDERS

ADAPTATION: SECURITY ACADEMY

Drivers:

- Increased demand for internal training
- DCSA Academy Definition
- Alignment with DCSA & Field
- Resourcing
- Position Changes

ST Enabling Support
Business Operations | Academic Support | Learning and Development

CDSE

Targeted Training Roles:
- Security Professionals and Practitioners
- General DOD Population
- Insider Threat Programs and Ops

DCSA Security Academy

Targeted Training Roles:
- DCSA Industrial Sec. Professionals
- DCSA Personnel Sec. Professionals
- DCSA CI Professionals
- Related Professionals

Integrated

NCCA

Targeted Training Roles:
- Federal polygraph professionals
- Credibility assessment policy advisors

Goal #1
Establish a DCSA Academy for Gatekeepers

Goal #2
Create Efficiencies via Common Functions

1 Security training is a key component of helping industry combat threats and assess organizational risk.

2 Trainings will ensure consistency for IS representatives in the field, across various regions.

3 Integrated training is offered for both industrial and personnel security representatives, as well counterintelligence professionals.

4 The DCSA Security Academy will complement curricula offered through CDSE and NCAA.

SECURITY TRAINING

CHANGE: SECURITY STANDARDS UPDATE

ADAPTATION: TOOLKITS FOR EASY REFERENCE

DCSA and the Center for Development of Security Excellence offer comprehensive toolkits that can significantly enhance the security posture of Federal Civilian Executive Branch agencies and the DoD.

Challenge	Solution	Relevant CDSE Toolkit
Lack of Awareness and Training	Regular training, phishing simulations, clear policies	Security Awareness Hub
Resource Constraints	Prioritize risks, leverage open-source tools, consider managed services	Industrial Security Toolkit
Complex Regulatory Requirements	Compliance management tools, expert consultation, regular audits	Compliance Toolkit
Integration with Existing Systems	Phased implementation, interoperability standards, vendor support	Cybersecurity Toolkit
Evolving Threat Landscape	Threat intelligence, continuous monitoring, regular updates	Threat Awareness Toolkit
Insider Threats	Access controls, behavior monitoring, whistleblower programs	Insider Threat Toolkit
Balancing Security and Usability	User-centric design, single sign-on (SSO), feedback loops	Cybersecurity Toolkit
Third-Party Risks	Vendor assessments, contractual obligations, continuous monitoring	Supply Chain Toolkit

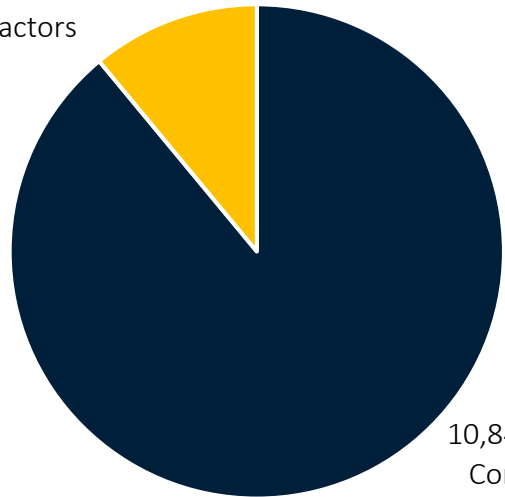# COUNTERINTELLIGENCE AND INSIDER THREAT

CHANGE: SUSPICIOUS CONTACT REPORT RATES

ADAPTATION: REPORTING A GREATER VOLUME OF CAGE CODES

Suspicious Activity Reporting FY 24

1,342 Cleared Contractors

- CCs That Have Not Submitted Reports
- CCs That Have Submitted Reports

10,849 Cleared Contractors

1 Counterintelligence improves mission execution and integration in the field to meet mandated requirements.

2 In FY 24, 1,342 unique cleared contractors submitted Suspicious Contact Reports.

3 Also in FY 24, between 10-11% of the NISP provided 100% of all reporting. Since then, the number of suspicious contact reports has doubled.

CLOSEOUT

**DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY**

UPCOMING EVENTS

1   **DCSA Virtual Security Conference: April 22-23**

2   **NISP Signatory Workshop: May 8**

3   **Industry Stakeholder Advisory board: May 20**

4   **NCMS Annual Seminar: June 10-12**

5   **DCSA Annual FOCI Conference: August 15**

**DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY**

HELPFUL RESOURCES

🔗 AGENCY LINKS

- Center for Development of Seurity Excellence: https://www.dcsa.mil/Security-Training/Center-for-Development-of-Security-Excellence-CDSE/
- DCSA Homeage: https://www.dcsa.mil/
- IS Main Page: https://www.dcsa.mil/Industrial-Security/
- National Background Investigation Services: https://www.dcsa.mil/Systems-Applications/National-Background-Investigation-Services-NBIS/
- FOCI Tools and Resources: https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Foreign-Ownership-Control-or-Influence/FOCI-Tools-Resources/
- Counterintelligence and Insider Threat: https://www.dcsa.mil/About-Us/Directorates/Counterintelligence-and-Insider-Threat/

🔗 EXTERNAL LINKS

- NISP and NISPPAC: https://www.archives.gov/isoo/oversight-groups/nisp
- NISP Operating Manual: https://www.federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-program-operating-manual-nispom
- National Security Agency: https://www.nsa.gov/
- Department of Defense Cyber Crime Center: https://www.dc3.mil/
- FBI Counterintelligence: https://www.fbi.gov/investigate/counterintelligence
- 32 CFR Part 117: https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117
- Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/

THIS IS PERSONAL TO ME

Confidence to defend the nation begins with DCSA:

- Industrial Security (IS) Classified: Frequency Hopping FM Radio

- IS Classified: EW Signal Jammer to protect against RF IED

- IS Classified: BLUE FORCE TRACKER command and control

- IS Classified: SATCOM radio for long range communication

- IS CUI: Production techniques for bullet proof windshield

- IS Classified: Cold rolled steel plate vehicle armor

- Personnel Security (PS) Background Investigation: Certified 17 years of periodic TS investigations

- IS Arms, Ammunition, and Explosives: Certified production for Rifle/ Side Arm/ Ammo Basic Load

- Security Training: Certified leaders in OPSEC/ INFOSEC/ PERSEC/ CYBER/ PHYSEC

- IS CUI: Production techniques for Ceramic body armor plates rated to 7.62 mm

- PS Adjudicators: Assessed trustworthy compliance and issued TS Clearances for over 17

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

OPEN DISCUSSION

**DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY**

THANK YOU

**DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY**