2021 JOINT NDIA/AIA FALL INDUSTRIAL SECURITY CONFERENCE

November 8 – 10 | Chantilly, VA | NDIA.org/ISCFall

TABLE OF CONTENTS

WHO WE ARE 2

SCHEDULE AT A GLANCE 2

EVENT INFORMATION 5

VENUE MAP 6

AGENDA 7

BIOGRAPHIES 14

SPONSORS 16

WHO WE ARE

The National Defense Industrial Association is the trusted leader in defense and national security associations. As a 501(c)(3) corporate and individual membership association, NDIA engages thoughtful and innovative leaders to exchange ideas, information, and capabilities that lead to the development of the best policies, practices, products, and technologies to ensure the safety and security of our nation. NDIA's membership embodies the full spectrum of corporate, government, academic, and individual stakeholders who form a vigorous, responsive, and collaborative community in support of defense and national security. For more than 100 years, NDIA and its predecessor organizations have been at the heart of the mission by dedicating their time, expertise, and energy to ensuring our warfighters have the best training, equipment, and support. For more information, visit **NDIA.org**

AIA AEROSPACE INDUSTRIES ASSOCIATION
100 YEARS

WHO WE ARE

The Aerospace Industries Association (AIA) was founded in 1919 and is the largest and oldest U.S. aerospace and defense trade association, representing 347 aerospace and defense manufacturers and suppliers with approximately 844,000 employees. Our members represent the leading manufacturers and suppliers of civil, military and business aircraft, missiles, space systems, aircraft engines, material and related components, equipment services and information technology. Visit **aia-aerospace.org** for more information.

SCHEDULE AT A GLANCE

MONDAY, NOVEMBER 8

PM Industry-Only Sessions
Grand Dominion Ballroom
12:30 - 3:25 pm

Breakout Sessions
Multiple Locations
3:35 - 5:45 pm

Networking Reception
Sunset Terrace
6:00 - 7:30 pm

TUESDAY, NOVEMBER 9

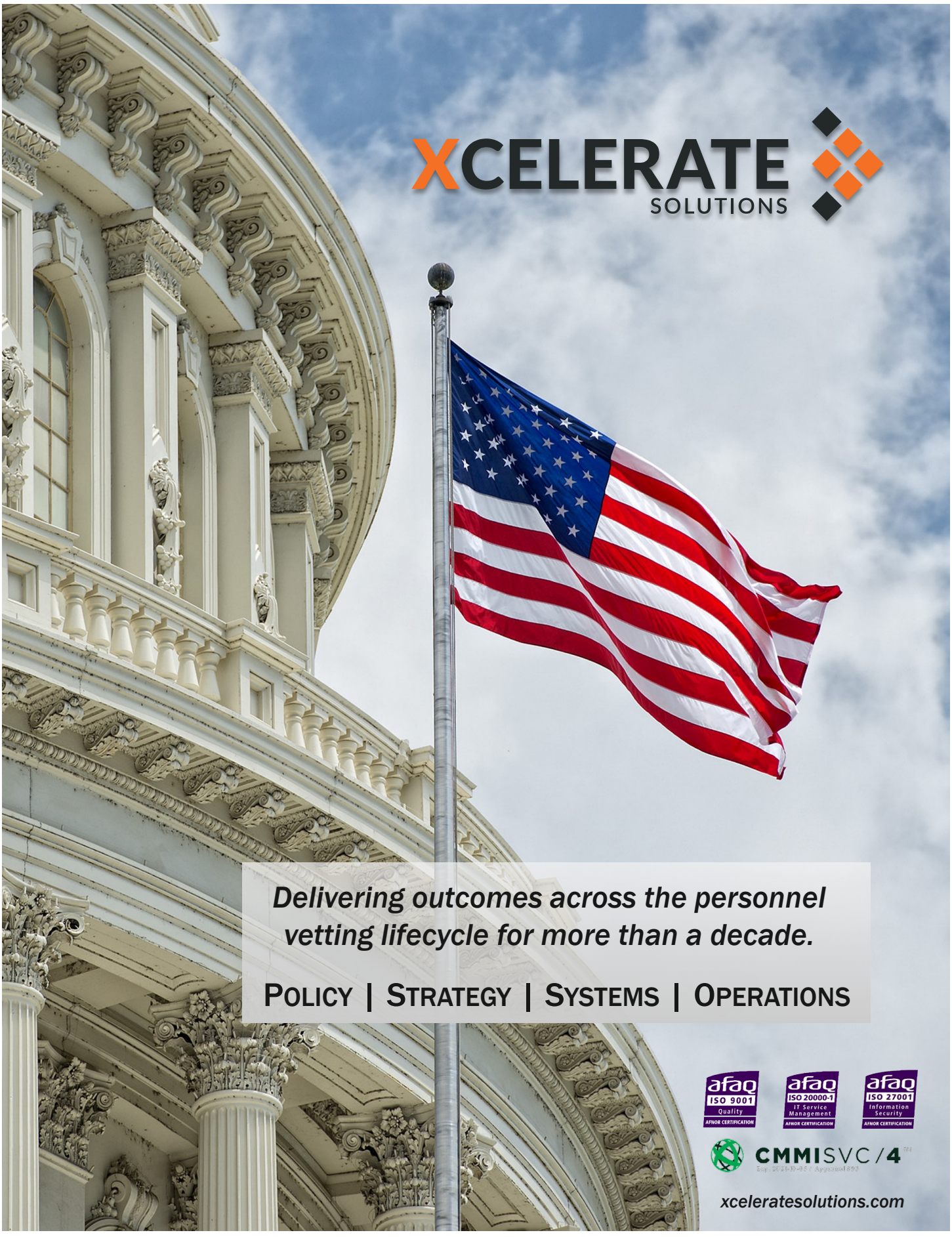
General Session
Grand Dominion Ballroom
8:15 am - 3:55 pm

Breakout Sessions
Multiple Locations
4:00 - 5:00 pm

Networking Dinner
Washingtonian Ballroom
7:00 - 9:00 pm

WEDNESDAY, NOVEMBER 10

General Session
Grand Dominion Ballroom
8:15 am - 5:15 pm


XCELERATE
SOLUTIONS
Delivering outcomes across the personnel vetting lifecycle for more than a decade.
POLICY | STRATEGY | SYSTEMS | OPERATIONS
afaq ISO 9001 Quality AFNOR CERTIFICATION
afaq ISO 20000-1 IT Service Management AFNOR CERTIFICATION
afaq ISO 27001 Information Security AFNOR CERTIFICATION
CMMISVC/4
xceleratesolutions.com

WELCOME TO THE 2021 JOINT NDIA/AIA FALL INDUSTRIAL SECURITY CONFERENCE

As your co-hosts, we would like to take this opportunity to welcome each and every one of you back to the first in-person joint NDIA/AIA Industrial Security Committee meeting since 2019! This meeting is the primary engagement forum for senior civilian U.S. Government industrial security policy makers from the Department of Defense and Intelligence Communities, as well as senior industry security executives from the top 200 defense companies. The planning committee members, as well as the many industry volunteers, have strived to create an agenda to provide you with the opportunity to engage with your government and industry counterparts in candid and respectful discussions on those strategic operational and policy issues directly impacting national security and mission success.

Over the next two and half days, the goal is to facilitate strong government and industry partnerships that can develop implementable solutions to address the critical issues and needs directly impacting government and industry. This meeting can only be as successful as you make it; your involvement is critical. Remember this meeting is a non-attributional environment, so please do not be shy. We look forward to meeting everyone. If there is anything we can do for you, please do not hesitate ask.

Enjoy the meeting.

Michelle Sutphin
Chair, Security & Counterintelligence Division, NDIA
Chief Security Officer, Science Applications International Corporation

Kai Hanson
Chair, Industrial Security Committee, AIA
Director, Global Security Programs, Collins Aerospace

GET INVOLVED
Learn more about NDIA's Divisions and how to join one at **NDIA.org/Divisions**

LEADERSHIP AND COMMITTEES

Michelle Sutphin
Division Chair

Quinton Wilkes
Division Vice Chair

SECURITY & COUNTERINTELLIGENCE DIVISION

WHO WE ARE

The Security & Counterintelligence Division—formerly the Industrial Security Committee of the Procurement Division—represents member companies' interests in all matters regarding industrial security. It is responsible for monitoring all security matters relating to the Defense Industrial Security Program, special access programs, and other activities that affect national security programs and corporate assets.

EVENT INFORMATION

LOCATION

Westfields Marriott Washington Dulles
14750 Conference Center Drive
Chantilly, VA 20151

ATTIRE

Civilian: Business
Military: Uniform of the Day

SURVEY AND PARTICIPANT LIST

You will receive via email a survey and list of participants (name and organization) after the conference. Please complete the survey to make our event even more successful in the future.

EVENT CONTACT

Andrea Lane, CMP, DES
Meeting Manager
(703) 247-2554
alane@NDIA.org

Jacqueline Dupre
Coordinator, Divisions
(703) 247-2575
jdupre@NDIA.org

Kirkland Dickson
Coordinator, Divisions
(703) 247-9479
kdickson@NDIA.org

PLANNING COMMITTEE

Michelle Sutphin
Chair, Security and Counterintelligence Division, NDIA

Quinton Wilkes
Vice Chair, Security and Counterintelligence Division, NDIA

Kai Hanson
Chair, Industrial Security Committee, AIA

Lisa Reidy
Vice Chair, Industrial Security Committee, AIA

SPEAKER GIFTS

In lieu of speaker gifts, a donation is being made to the Fisher House Foundation.

HARASSMENT STATEMENT

NDIA is committed to providing a professional environment free from physical, psychological and verbal harassment. NDIA will not tolerate harassment of any kind, including but not limited to harassment based on ethnicity, religion, disability, physical appearance, gender, or sexual orientation. This policy applies to all participants and attendees at NDIA conferences, meetings and events. Harassment includes offensive gestures and verbal comments, deliberate intimidation, stalking, following, inappropriate photography and recording, sustained disruption of talks or other events, inappropriate physical contact, and unwelcome attention. Participants requested to cease harassing behavior are expected to comply immediately, and failure will serve as grounds for revoking access to the NDIA event.

EVENT CODE OF CONDUCT

NDIA's Event Code of Conduct applies to all National Defense Industrial Association (NDIA), National Training & Simulation Association (NTSA), and Women In Defense (WID) meeting-related events, whether in person at public or private facilities, online, or during virtual events. NDIA, NTSA, and WID are committed to providing a productive and welcoming environment for all participants. All participants are expected to abide by this code as well as NDIA's ethical principles and practices. Visit NDIA.org/CodeOfConduct to review the full policy.

REAL-TIME Q&A

Slido is an audience engagement platform that allows users to crowd-source top questions to drive meaningful conversations and increase crowd participation. Participants can up-vote the questions they would most like to hear discussed. Simply tap the thumbs-up button to up-vote a question. Top questions are displayed for the moderator and speaker to answer.

Event code: **#ISCFALL**

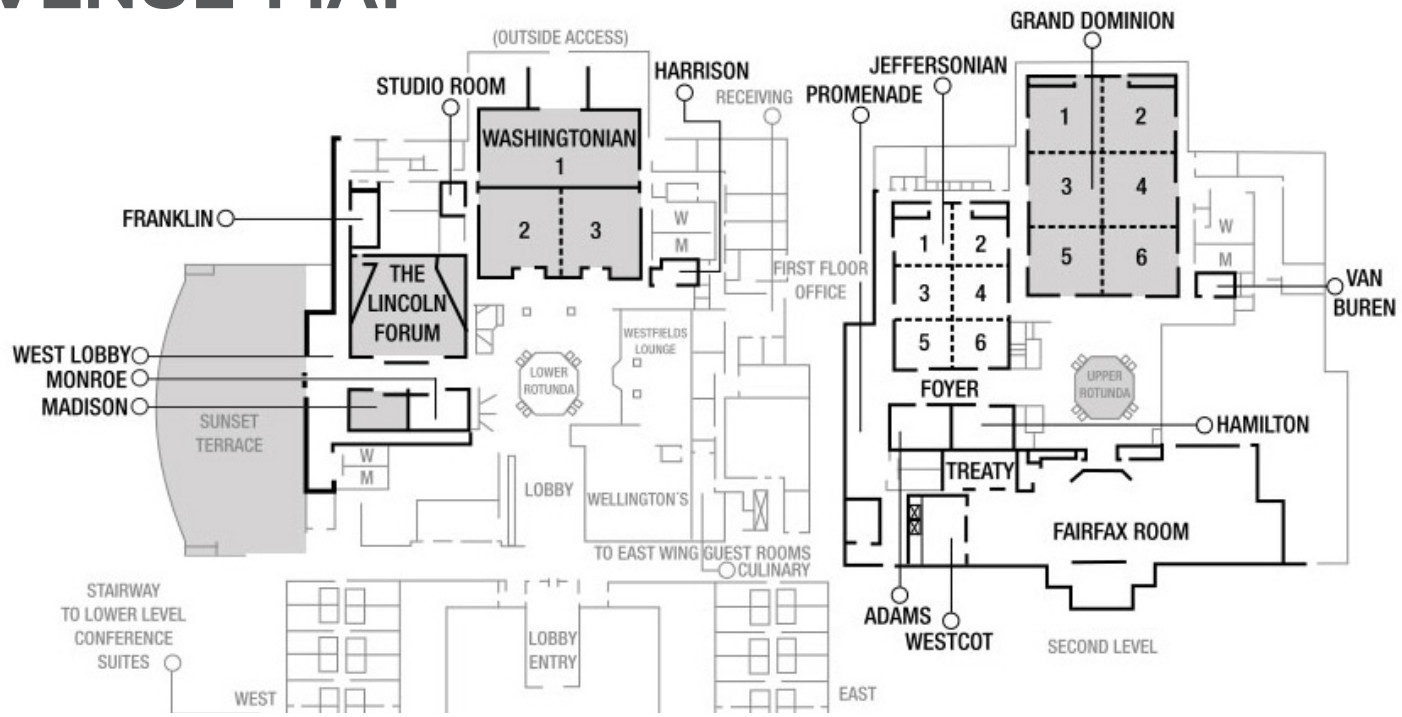
MOBILE APP

Make the most of your attendance at the 2021 Joint NDIA/AIA Fall Industrial Security Conference with the NDIA Events mobile app, available on the App Store for Apple devices and Google Play for Android devices. Simply search "NDIA Meetings" to find and download the NDIA Events app for free. With it, you will have 24/7 access to an activity feed, speaker listings, sponsor and exhibitor information, Sli.do, and venue maps. Be sure to accept push notifications so that you can receive the most up-to-date information regarding any changes to the forum agenda.

ANTITRUST STATEMENT

The NDIA has a policy of strict compliance with federal and state antitrust laws. The antitrust laws prohibit competitors from engaging in actions that could result in an unreasonable restraint of trade. Consequently, NDIA members must avoid discussing certain topics when they are together at formal association membership, board, committee, and other meetings and in informal contacts with other industry members: prices, fees, rates, profit margins, or other terms or conditions of sale (including allowances, credit terms, and warranties); allocation of markets or customers or division of territories; or refusals to deal with or boycotts of suppliers, customers or other third parties, or topics that may lead participants not to deal with a particular supplier, customer or third party.

VENUE MAP



AGENDA

MONDAY, NOVEMBER 8

8:00 am – 6:30 pm

REGISTRATION
GRAND DOMINION FOYER

10:00 – 11:00 am

EXCOMM MEETING
MADISON

PM INDUSTRY-ONLY SESSIONS

12:30 – 12:40 pm

OPENING REMARKS
GRAND DOMINION BALLROOM

Michelle Sutphin
Chair, Security & Counterintelligence Division, NDIA
Chief Security Officer, Science Applications International Corporation

Kai Hanson
Chair, Industrial Security Committee, AIA
Director, Global Security Programs, Collins Aerospace

12:40 – 1:55 pm

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COUNCIL (NISPPAC) PANEL
GRAND DOMINION BALLROOM

Heather Sims
NISPPAC, Industry Spokesperson, L3Harris
Moderator

Aprille Abbott
Corporate Security Manager, The MITRE Corporation

Rosael Borrero
Senior Cloud Cybersecurity Engineer, Team Lead, Special Aerospace Security Services, Inc.

Derek Jones
Assistant Department Head – Government Security, Security Services Department, MIT Lincoln Laboratory

Tracy Durkin
Vice President, Security, ManTech

David Tender
Senior Vice President, Chief Security Officer, ASRC Federal

1:55 – 2:25 pm

NETWORKING BREAK
UPPER ROTUNDA

2:25 – 3:25 pm

LEGISLATIVE DISCUSSION PANEL

GRAND DOMINION BALLROOM

Jon Rosenwasser
Budget & Policy Director, U.S. Senate

Chris Howell
Professional Staff Member, U.S. Senate

CONCURRENT BREAKOUT SESSIONS

3:35 – 4:35 pm

NDIA Membership Meeting

GRAND DOMINION BALLROOM

Michelle Sutphin
Chair, Security & Counterintelligence Division, NDIA
Chief Security Officer, Science Applications International Corporation

AIA Membership Meeting

WASHINGTONIAN 2 - 3

Kai Hanson
Chair, Industrial Security Committee, AIA
Director, Global Security Programs, Collins Aerospace

4:45 – 5:45 pm

Joint Cyber Intelligence Tool Suite (JCITS)

GRAND DOMINION BALLROOM

Randy Newman
Deputy Assistant Director, Cyber Capabilities Integration, Naval Criminal Investigative Service

Jay Kearney
Chief, Strategy and Engagement Branch, Cyber Division, Counterintelligence Directorate, Defense Counterintelligence and Security Agency

DCSA Regional Directors & VRO

WASHINGTONIAN 2-3

Justin Walsh
Capitol Regional Director, Defense Counterintelligence and Security Agency

Heather Green
Assistant Director, Vetting Risk Operations, Defense Counterintelligence and Security Agency

Keith Minard, CTP
Senior Policy Advisor, Defense Counterintelligence and Security Agency

Booker Bland, CTP
Deputy Senior Policy Advisor, Defense Counterintelligence and Security Agency

DCSA Authorization Office

LINCOLN FORUM

David Scott
NISP Authorizing Official, Critical Technology Protection, Defense Counterintelligence and Security Agency

6:00 – 7:30 pm

NETWORKING RECEPTION

SUNSET TERRACE

TUESDAY, NOVEMBER 9

7:00 am – 7:00 pm

REGISTRATION
GRAND DOMINION FOYER

7:00 – 8:00 am

NETWORKING BREAKFAST
WASHINGTONIAN BALLROOM

FULL SESSION (INDUSTRY & GOVERNMENT)

8:15 – 8:25 am

OPENING REMARKS
GRAND DOMINION BALLROOM

Michelle Sutphin
Chair, Security & Counterintelligence Division, NDIA
Chief Security Officer, Science Applications International Corporation

Kai Hanson
Chair, Industrial Security Committee, AIA
Director, Global Security Programs, Collins Aerospace

8:25 – 9:25 am

NATIONAL COUNTERINTELLIGENCE SECURITY CENTER UPDATE

GRAND DOMINION BALLROOM

Michael Orlando
Acting Director, National Counterintelligence and Security Center

9:30 – 10:15 am

OFFICE OF THE UNDER SECRETARY FOR DEFENSE (INTELLIGENCE) (OUSD(I)) SECURITY UPDATE

GRAND DOMINION BALLROOM

Garry Reid
Director for Defense Intelligence, Counterintelligence, Law Enforcement & Security, OUSD(I)

10:15 – 10:45 am

NETWORKING BREAK

UPPER ROTUNDA

10:45 – 11:45 am

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DCSA) UPDATE

GRAND DOMINION BALLROOM

William Lietzau
Director, Defense Counterintelligence and Security Agency

11:45 am – 1:15 pm

LUNCH (ON YOUR OWN)

1:15 – 1:25 pm

OPENING REMARKS

GRAND DOMINION BALLROOM

Michelle Sutphin
Chair, Security & Counterintelligence Division, NDIA
Chief Security Officer, Science Applications International Corporation

Kai Hanson
Chair, Industrial Security Committee, AIA
Director, Global Security Programs, Collins Aerospace

1:25 – 2:25 pm

CONTROL RISKS: INTERNATIONAL THREAT UPDATE

GRAND DOMINION BALLROOM

Jonathan Wood
Principal, Global Issues Group, Control Risks

2:25 – 2:55 pm

NETWORKING BREAK

UPPER ROTUNDA

2:55 – 3:55 pm

TRUSTED WORKFORCE 2.0 PANEL

GRAND DOMINION BALLROOM

Matt Eanes
PAC PMO Director, Security, Suitability, & Credentialing, Performance Accountability Council

Heather Green
Assistant Director, Vetting Risk Operations, Defense Counterintelligence and Security Agency

Heather Sims
NISPPAC, Industry Spokesperson, L3Harris

3:55 pm

ADJOURN FOR THE DAY

CONCURRENT BREAKOUT SESSIONS

4:00 – 5:00 pm

Foreign Ownership, Control or Influence (FOCI) Roundtable

GRAND DOMINION BALLROOM

Jennifer Brown
Senior Director, Corporate Security, iDirect Government

Dustin Dwyer
Chief of Mitigation Strategy Unit, Defense Counterintelligence and Security Agency

Air Force Special Access Program (SAP) Roundtable

WASHINGTONIAN 2- 3

Terry Phillips
Special Access Program Security Director, U.S. Air Force

Col William MacLure, USAF (Ret)
Director, Security, Special Program Oversight and Information Protection, U.S. Air Force

7:00 – 9:00 pm

NETWORKING DINNER

WASHINGTONIAN BALLROOM

WEDNESDAY, NOVEMBER 10

7:00 am – 5:00 pm

REGISTRATION
GRAND DOMINION FOYER

7:00 – 8:00 am

NETWORKING BREAKFAST
WASHINGTONIAN BALLROOM

FULL SESSION (INDUSTRY & GOVERNMENT)

8:15 – 8:25 am

OPENING REMARKS
GRAND DOMINION BALLROOM

Michelle Sutphin
Chair, Security & Counterintelligence Division, NDIA
Chief Security Officer, Science Applications International Corporation

Kai Hanson
Chair, Industrial Security Committee, AIA
Director, Global Security Programs, Collins Aerospace

8:25 – 9:25 am

RANSOMWARE LESSONS LEARNED
GRAND DOMINION BALLROOM

Kyriakos Vassalakos
Supervisory Special Agent, Federal Bureau of Investigation, Washington Field Office

David Clow
Chief Information Officer, Metropolitan Police Department of the District of Columbia

9:25 – 9:55 am

NETWORKING BREAK
UPPER ROTUNDA

9:55 – 10:55 am

IC DIRECTORS PANEL
GRAND DOMINION BALLROOM

Jamie Clancy
Chief, Office of Security and Counterintelligence, National Reconnaissance Office

CAPT Scott Minke, USNR (Ret)
Deputy Chief Personnel Security, Office of Security, Defense Intelligence Agency

Jeremy Sansbury
Chief of Security and Counterintelligence, National Security Agency

Doug Van Zandt
Director of Security, Central Intelligence Agency

11:00 am – 12:00 pm

SAP PANEL

GRAND DOMINION BALLROOM

Kristinia Glines
Director of Security, Department of Navy Special Access Programs Central Office

Terry Phillips
Special Access Programs Security Director, U.S. Air Force

Lee Russ
Director, Counterintelligence and Global Special Access Programs, Department of Defense Special Access Programs Central Office

Brandon Winder
Security Director, U.S. Army Special Access Programs Central Office

12:00 – 1:30 pm

LUNCH (ON YOUR OWN)

1:30 – 2:30 pm

CUI SPEAKER

GRAND DOMINION BALLROOM

John Massey
Deputy Assistant Director, Enterprise Security Operations, Critical Technology Protection, Defense Counterintelligence and Security Agency

2:35 – 3:35 pm

C-SUITE PANEL

GRAND DOMINION BALLROOM

Alice Eldridge
Senior Vice President & General Counsel, BAE Systems

Mark Escobar
Senior Vice President & Chief of Business Operations, SAIC

Charlie Sowell
Chief Executive Officer, SE&M Solutions, LLC

3:35 – 4:05 pm

NETWORKING BREAK

UPPER ROTUNDA

4:05 – 5:05 pm

CHINA-CHANGING THE SUPPLY CHAIN

GRAND DOMINION BALLROOM

Levi Thomas
Special Agent, Federal Bureau of Investigation, Washington Field Office

5:05 – 5:15 pm

CLOSING REMARKS

GRAND DOMINION BALLROOM

Michelle Sutphin
Chair, Security & Counterintelligence Division, NDIA
Chief Security Officer, Science Applications International Corporation

Kai Hanson
Chair, Industrial Security Committee, AIA
Director, Global Security Programs, Collins Aerospace

BIOGRAPHIES

WILLIAM LIETZAU

Director
Defense Counterintelligence and Security Agency

William K. Lietzau is the Director of the Defense Counterintelligence and Security Agency (DCSA).

In this capacity, Mr. Lietzau leads both the personnel vetting and critical technology protection missions under DCSA and manages approximately 12,000 federal and contract support personnel worldwide. Additionally, Mr. Lietzau directs the development of an end-to-end national-level Information Technology infrastructure designed to support the personnel vetting enterprise.

Prior to his current role, Mr. Lietzau served as the Director of the Personnel Vetting Transformation Office where he managed the transfer of the National Background Investigations Bureau (NBIB) to the nascent Defense Counterintelligence and Security Agency (DCSA), and initiated and led associated transformational efforts.

Before returning to government, Mr. Lietzau was Vice President at a large government services contractor where he initially served as Deputy General Counsel overseeing security, contracting, international trade and compliance. He later became general manager of an international business unit providing counter-terrorism and law enforcement training and mentoring in over 35 countries as well as related O&M, minor construction, and security services.

Mr. Lietzau served over three years as Deputy Assistant Secretary of Defense for Rule of Law and Detainee Policy and on several U.S. delegations negotiating multilateral treaties. A retired Marine Corps Colonel, he served 27 years as an infantry officer and then judge advocate, commanding at the company, battalion, and installation levels. An expert in international law, he also served as a prosecutor, defense counsel and judge and provided legal advice at a combatant command, the Joint Staff, the Office of the Secretary of Defense, and the National Security Council.

Mr. Lietzau received a Bachelor of Science from the United States Naval Academy and his Juris Doctorate from Yale Law School. He also holds an LL.M. from the U.S. Army Judge Advocate General's School, and a Master of Science in National Security Studies from the National War College.

MICHAEL ORLANDO

Acting Director
National Counterintelligence and Security Center

Michael J. Orlando is a Senior Executive Service leader with more than 25 years of law enforcement, Intelligence Community, and military experience, including counterintelligence and counterterrorism investigations. Mr. Orlando joined the National Counterintelligence and Security Center in November, 2020, serving in the position of Deputy Director.

Mr. Orlando recently served as a Deputy Assistant Director in the Counterterrorism Division in the Federal Bureau of Investigation (FBI). In that capacity, he was responsible for overseeing the business administration and operational support for the division, which included technology development, human resource matters, financial management, and private-sector partner engagements. Mr. Orlando also served as the acting head of the Counterterrorism Division and successfully managed several interagency crisis incident responses, including the attack at Pensacola Naval Air Station; Manda Airstrip, Kenya; as well as domestic terrorism attacks in Jersey City, NJ, and Monsey, NY.

Mr. Orlando served as an FBI Special Agent in 2003 and was assigned to the Pittsburgh Division where he investigated counterintelligence matters. In his follow-on field assignment to the Washington Field Office, he worked on high priority counterintelligence special projects with multiple deployments to the People's Republic of China. In 2009, Mr. Orlando was the program manager assigned to an FBI task force where he coordinated counterintelligence operations in the Western Pacific and East Asia and led an interagency and foreign partner effort to disrupt foreign influence in the region.

In 2011, Mr. Orlando returned to the field and was assigned to the Honolulu Field Office where he oversaw the successful espionage investigation and conviction of a DoD contractor for passing national defense secrets to China. In 2013, Michael served as the principal deputy for the East Asia Section in the Counterintelligence Division, and in 2017 he served as Assistant Special Agent in Charge of the Washington Field Office, Counterintelligence Division, where he oversaw the successful disruption of Russian clandestine foreign agent Maria Butina. In 2018, he helped create the Counterterrorism Division's Iran Threat Task Force, now the Iran Mission Center, as its first Acting Section Chief.

Mr. Orlando has received the FBI Director's Award for Outstanding Counterintelligence Investigation and has been awarded three Director of National Intelligence awards for Counterintelligence Operations.

A native of New York, Mr. Orlando received his bachelor's degree in Economics and Management from the State University of New York, College at Cortland. In 2017, Michael attended Georgetown University's McDonough School of Business and earned a master's in leadership. Prior to working for the FBI, he was an officer in the U.S. Army and was employed by the Central Intelligence Agency.

GARRY REID

Director for Defense Intelligence (Counterintelligence, Law Enforcement and Security)
Office of the Under Secretary of Defense for Intelligence & Security

Garry Reid serves as the Director for Defense Intelligence (CL&S) reporting directly to the Under Secretary of Defense for Intelligence and Security (USD(I&S)). In this capacity, he is responsible for the formulation and implementation of policy and resources to conduct counterintelligence, law enforcement, and security programs. Previous assignments include Senior Advisor to the USD(I) and the Director for Defense Intelligence (Intelligence & Security).

Mr. Reid previously served in the Office of the Under Secretary of Defense for Policy as the Principal Deputy Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, and as the Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism, where he advised the Assistant Secretary, the Under Secretary, and the Secretary of Defense on policies, plans, authorities, and resources related to special operations and irregular warfare.

Mr. Reid retired from the U.S. Army in 2005.

HEATHER SIMS

National Industrial Security Program Policy Advisory Council (NISPPAC), Industry Spokesperson
L3Harris

Mrs. Heather Sims provides Strategic Industrial Security advice for the Chief Security Officer at L3Harris, headquartered in Melbourne, Florida. Her primary responsibility is to provide subject matter expertise for a variety of security disciplines throughout the L3Harris enterprise.

Ms. Sims is also the current Industry Spokesperson to the National Industrial Security Program Policy Advisory Committee (NISPPAC). NISPPAC members advise on all matters concerning the policies of the National Industrial Security Program, including recommending changes. The NISPPAC serves as a forum to discuss policy issues in dispute.

Prior to her arrival at L3Harris, Mrs. Heather Sims was the Strategic Security Advisor to the General Dynamics Chief Security Officer. Prior to her arrival in cleared industrial, Heather was the Assistant Deputy Director for Industrial Security Field Operations at the former Defense Security Service, now Defense Counterintelligence and Security Agency located in Quantico, Virginia. Mrs. Sims was responsible for the day-to-day field operations throughout the United States and was an instrumental liaison to other government agencies and cleared contractors. Prior to assuming the role of Assistant Deputy Director, she was the St. Louis Field Office Chief, responsible for supporting approximately 700 facilities in Missouri, Illinois, Wisconsin, Indiana, Minnesota, and Iowa. Mrs. Sims last role with DSS was a special Department of Defense project on behalf of the Secretary of Defense researching and preparing a Congressional response to The National Defense Authorization Act for Fiscal Year 2017 Section 951, ultimately bringing the security investigation mission back to the department for the federal government.

Prior to her employment with DSS, Mrs. Sims was the Chief, Plans and Programs, 375 Security Forces Squadron, Scott Air Force Base, Illinois. Mrs. Sims provided supervision to over 27 staff personnel comprised of civilian, military and contractors. She had program management oversight of the following: Police Service, Installation Security, Physical Security, Electronic Security Systems, Policy and Plans, Installation Constable, Reports and Analysis and Information/Industrial/Personnel Security at an Air Force installation that was home to USTRANSCOM, Headquarters Air Mobility Command, Air Force Communications Agency and three Air Force wings Additionally, Mrs. Sims was responsible for security oversight of 64 geographically separate units across the United States.

Mrs. Sims holds a Bachelor's degree in Workforce Education and Development from the University Southern Illinois. She is a graduate of the Excellence in Government Senior Fellows Program and the Federal Executive Institute as well as a recipient of the Distinguished Service Award and the Air Force Exemplary Civilian Service award. Mrs. Sims grew up in Pennsylvania and began her Air Force career in August 1989 as a Law Enforcement Specialist. Following Law Enforcement technical training, she was assigned to various overseas and stateside assignments working a variety of law enforcement and security positions. She lives in Melbourne, Florida with her husband John Sims and two of their three children.

SPONSOR DESCRIPTIONS

XCELERATE SOLUTIONS Secure Results. Delivered.

Xcelerate Solutions (Xcelerate) is a mission-driven consultancy committed to enhancing America's personnel and cyber security posture. Its focus is, and always has been, to help make America safer by solving complex problems and accelerating results. Xcelerate delivers innovative solutions in three service areas: Enterprise Security, Strategic Consulting, and Digital Transformation. Leveraging these core capabilities, Xcelerate provides full lifecycle solutions, beginning with creation of a strategy aligned with client objectives and a roadmap to realize the strategy. Xcelerate's design, development, and integration capabilities, based on consulting and technology expertise, helps clients operationalize the plan. Xcelerate has deep experience in both traditional and Agile project management, as well as a proven ability to help traditional programs transition to an Agile Framework. Once a solution is implemented, Xcelerate provides consulting and IT services to ensure it operates as designed, driving mission critical, high-volume transactions and supporting customers with a focus on continuous improvement.

Xcelerate has leveraged its broad capabilities to support the end-to-end Security, Suitability, and Credentialing (SSC) Mission for over a decade. Through strategy, management, and operational services, they continue to play a key role in today's SSC modernization efforts.

An ISO 9001, ISO 20000-1, and ISO 27001 certified company, Xcelerate prides itself on delivering high-quality services to clients in accordance with CMMI-SVC Level 4 appraised process.

BABELSTREET

Babel Street is the world's leading AI-enabled data-to-knowledge company. The company's technology allows customers to rapidly discover and decipher the insights they need to empower their missions, regardless of origin, language or platform. Babel Street's patented analytics software transforms the most relevant insights for our customers through AI-enabled, cross-lingual, conceptual and persistent search of information from around the world. For more information, visit www.babelstreet.com.

Securitas

Securitas Critical Infrastructure Services (SCIS) and their subsidiary, Paragon Systems, employ over 14,000 professionals in specialized operations providing security, fire, investigations, inspections, cybersecurity, risk management, and mission support services to the U.S. Federal Government and other critical infrastructure clients. SCIS and Paragon are Safeguarding American Assets at home and abroad.

iWorks CORPORATION

iWorks is a leading provider of IT services, recognized in personnel security and vetting solutions, Agile, DevOps, DevSecOps, data analytics, and cloud solutions. We are certified CMMI Level 4, ISO 9001:2015, 20000-1:2011, and 27001:2013. iWorks is one of 34 CMMC Third Party Assessment Organizations and a certified Registered Provider Organization.

SIMS® SOFTWARE

SIMS Software is the leading software tool for security information management within the government and defense industries. SIMS includes 17 comprehensive modules with a fully automated view of information within your security domain. SIMS provides all tools needed for a powerful security program within a single system.

LexisNexis® RISK SOLUTIONS

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. Headquartered in Georgia and part of RELX, a global provider of information-based analytics and decision tools. https://risk.lexisnexis.com/law-enforcement-and-public-safety

KPMG

For 100+ years, KPMG has assisted the DoD with various services including Data & Analytics, Financial Management, Technology, Cybersecurity, Intelligent Automation, Digital Transformation, Supply Chain and more. We help clients adapt and transform their business models, better leverage data, increase operational efficiencies, and ensure greater transparency. www.kpmg.com/us/federal

TransUnion

Whether federal, state or local agency, public safety or educational organization, TransUnion's suite of mission-critical solutions provides the public sector with vital information and an unmatched combination of credit and non-credit data to help ensure citizen safety, manage compliance and boost services for constituents served. Visit https://www.transunion.com/industry/public-sector for more information.

THOMSON REUTERS
SPECIAL SERVICES

SE&M Solutions LLC

National Industrial Security Program Policy Advisory Committee (NISPPAC)

NISPPAC Industry Updates

November 2021 Update

"Approved for Public Release"

Industry's Role on the NISPPAC

- The NISPPAC was created 8 Jan 93, by Executive Order 12829, "NISP" Functions:
  - ✓ Advise the Chair of the Committee (ISOO, Director) on all NISP policies, including recommending changes
  - ✓ Serves as a forum to discuss policy issues in dispute.
- Comprised of 16 government and 8 industry members
- Two new industry members elected annually
- Nominations by current industry NISPPAC & MOU members
- Meets publicly at least twice a year
- Creates Working Groups covering several NISP topic areas
- Industry members represent ALL NISP companies (Small, Medium, Large, FFRDC/UARC, etc.) and not their own self-interest or company interest
- Industry members are skilled in NISP Functions

Who We Are

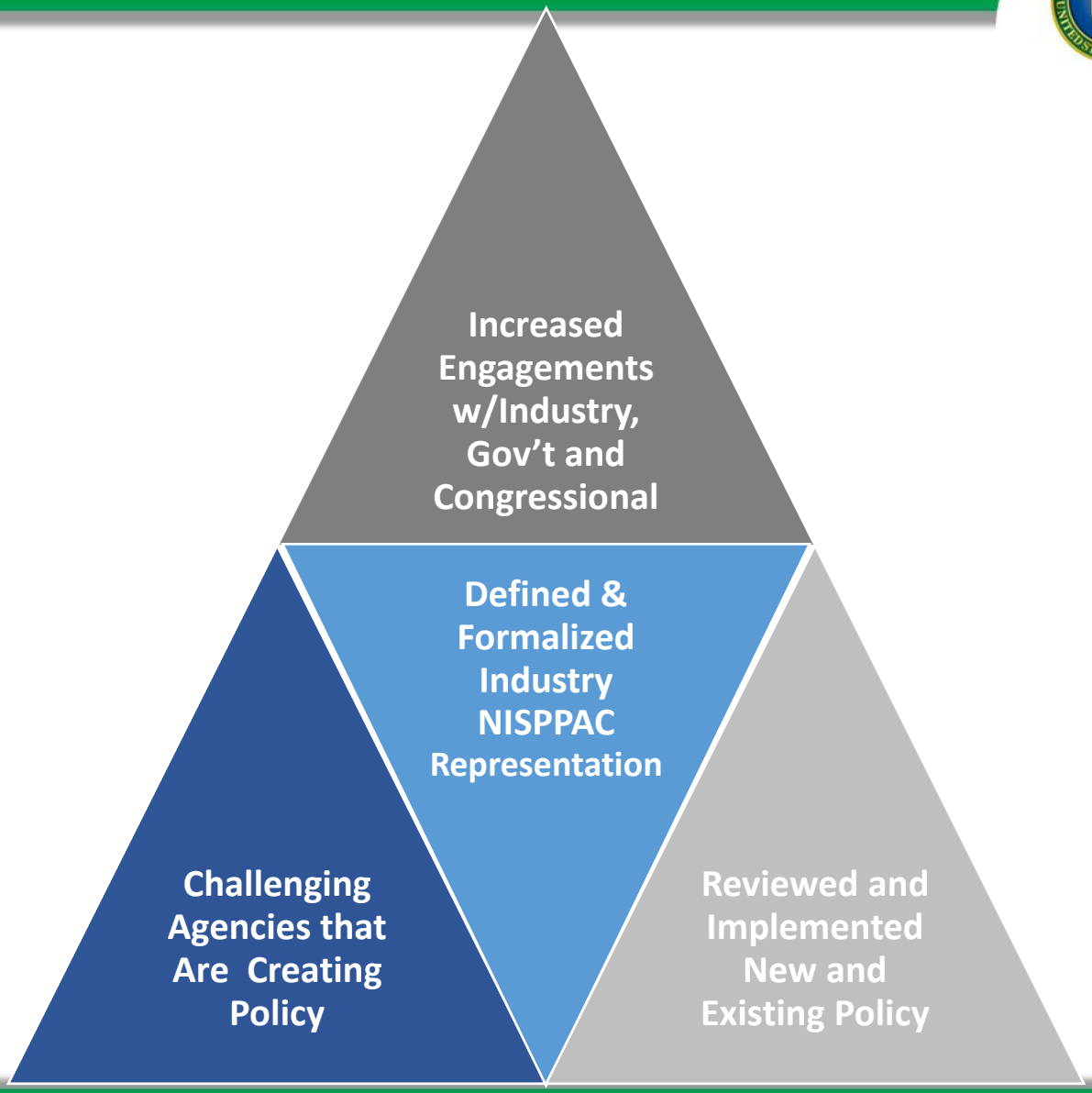
INDUSTRY	
Heather Sims, Spokesperson	L3Harris
Aprille Abbott	MITRE
Rosie Borrero	SASSI
Derek Jones	MIT Lincoln Labs
Dave Tender	ASRC Federal
Greg Sadler	GDIT
Tracy Durkin	Mantech
Cheryl Stone	RAND Corp

INDUSTRY MOU	
Kai Hanson	AIA
Jonathan Fitz-Enz	ASIS
Joe Kraus	CSSWG
Jordan Baxter	FFRDC/UARC
Kathy Pherson	INSA
Pending Elections	ISWG
Lynn Burns	NCMS
Michelle Sutphin	NDIA
Marc Ryan	PSC

For the most up to date member listing, refer to archieves.gov/isoo.oversight-groups/nisppac

The Last Two Years

Industry NISPPAC Efforts=2 Years



Strategic Industry NISPPAC Priorities

TWF 2.0

CUI/CMMC

RMF

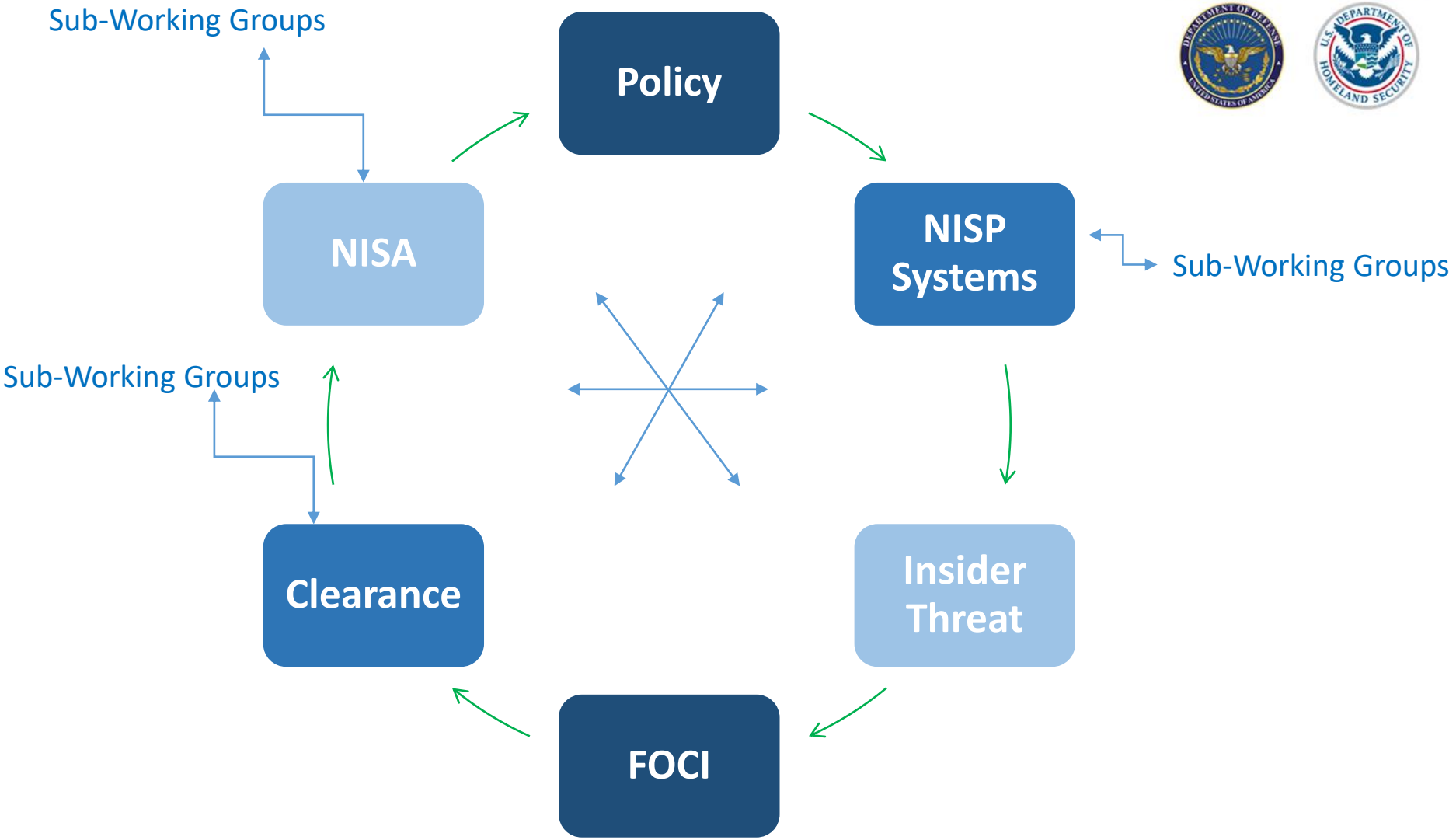
NISP Systems

CSA Processes/ Guidance

UNITING INDUSTRY'S VOICE

WORKING NISP ISSUES THROUGH FORMAL CHANNELS FOR IMPROVEMENT ACCOUNTABILITY

Current NISPPAC Working Groups



NISPOM Rule, 32 CFR, Part 117

- **Key Changes-How does it impact your company?**
  - SMO Duties-*applies to 100% of Cleared Companies*
  - Incorporation of SEAD 3 reporting requirements-*applies to 100%*
  - TS Accountability- *applies to less than 100 Cleared Companies*
  - IDS Installation- *applies to Cleared Companies that have IDS*
  - Safeguarding-*applies to less than 4000 of Cleared Companies*
  - Classified Information Retention-*applies to 100% Companies* that have safeguarding
  - Section 842 Public Law 115-232-Gov't-Foreign Companies w/Proscribed Information
  - Two Types of Limited FCLs-Gov't
  - Granting FCLs-Gov't
- **Tools**
  - List of major changes in the preamble of the Rule
  - Cross Reference Tool
  - CDSE Webinar and Other Engagements
  - DCSA updating tools, oversight guidance/rating system and NISP systems
  - CSAs provided their NISPOM implementation plans at the April Public NISPPAC Mtg
- **Recommendations for Industry**
  - ISL are not stand alone, READ and KNOW the POLICY
  - Make informed decisions
  - Use available tools
  - Ask for help/send in compliance interpretation concerns

National Level Policy Updates

- **SEADs-ODNI**
- **ISLs (not stand-alone documents)**
  - SEAD 3- Adverse Information Reporting
  - 32 CFR, Part 117
  - Usage of EPL List and Crosscut Shredders
  - Insider Threat
  - Top Secret Accountability
- **KMP Designation and SMO Training**
- **CUI/CMMC Implementation**
- **GSA Announcement of Black Label Phase Out (Black and silver label)**
  - Phase out of GSA approved security containers and Vault Doors manufactured prior to 1989
  - Phasing out from 1954-1989
  - Over a period of 4 years starting as of October 1, 2024

Clearance Working Group

- **Industry NISP Priorities/Watch List**
  - *NISPOM, 32 CFR, Part 117/SEAD 3*
    - Oversight-Compliance Updates from CSAs
    - What is reportable under SEAD 3?
    - SEAD 3 ISL-Foreign Travel
    - SMO training requirements
  - *TWF 1.5 and 2.0*
    - NBIS
      - Industry Requirements/Testing
      - Transition from DISS to NBIS
    - CV – 9/30 DNI Mandate
      - Current Process
      - Current Numbers Due to Be Compliant
  - FCL process and Timelines (Metrics)
  - New Self-Inspection Handbook
  - DCSA Org Chart and Leadership Roles

Insider Threat Working Group

1. Information Sharing
   - Items known by the Govt and sharing to Industry
   - All Security relevant information
   - May Cyber EO requires information sharing across Govt

2. DRAFT SEAD 9, Trusted Workforce, Whistleblower

3. SEAD 3 ISL Self Reporting
   - ✓ Consolidated Reporting for multiple agencies
   - ✓ Reporting to CISA and ISRs?
   - ✓ Adverse Information Reporting

4. Insider Threat Policy Implementation
   - How is the Govt measuring effectiveness?
   - Consistent Roll out

5. Mandatory COVID Immunization

NISP System Working Group

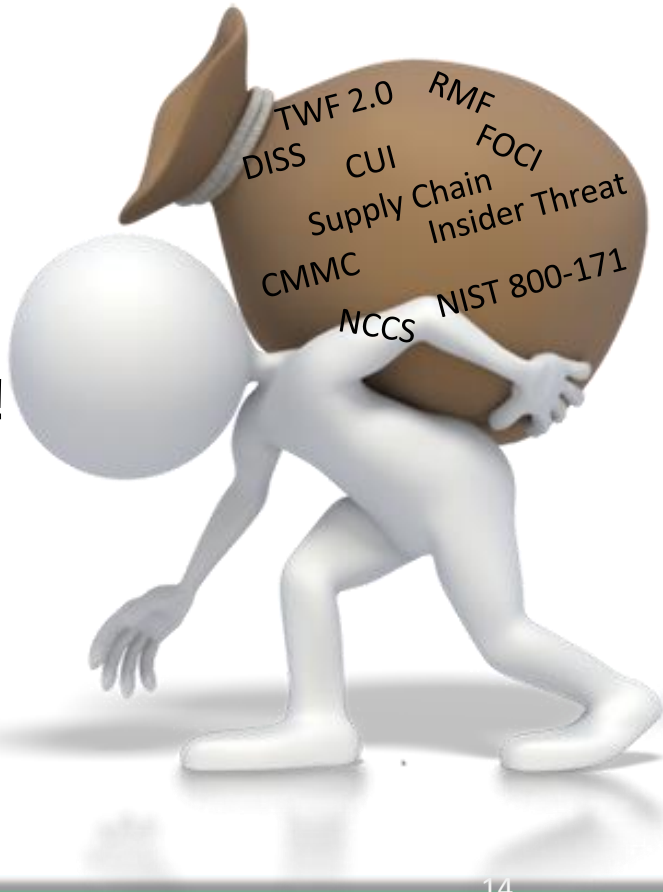
- Consists of 5 primary sub working groups
  - JPAS-DISS
    - Lead: Jeremy Wendell
  - NBIS/e-APP
    - Lead: Quinton Wilkes
  - NCCS
    - Lead: Gregory Sadler and Amber Elliott
  - NISS
    - Lead: Lisa Reidy
  - SWFT
    - Lead: Jonathan Fitz-Enz
  - Other CSA Systems
    - eMass: Scott Taylor has been providing a liaison between the NISA working group and DCSA
    - As the need arises for coordination of additional CSA systems

NISA Working Group

- Increased NAO/RAO Collaboration
- eMASS Package Workflow Enhancements (CY 22)
  - ✓ More transparent tracking of submissions/approval process
- RMF Package Approval Timelines
  - ✓ SCA Triage
- NISP Connection Process Guide
- Moving Forward.. Industry Priorities?

Evolving NISP
Understanding Impact to Industry

- Alignment/Unity of Industry on the Basics
- Read/Understand the Policies
- We don't have to ask DCSA permission for everything!
- Proactive Communication-Industry and Gov't
- What can we expect from our CSA?
- New/Bad Processes=New Industry Burden
- Engagement at all levels but at the right level!
- UTOPIA!!! Industry self ID issues & partner w/Gov't-Don't operate in Fear
- Approach when things are not working well!



Industry NISPPAC on the Web

https://classmgmt.com/nisppac.php

Industry NISPPAC by email

nisppacindustry@gmail.com

"Approved for Public Release"

QUESTIONS ???

CONTROLLED UNCLASSIFIED INFORMATION:

BUILDING YOUR STARTER CUI PROGRAM

2021 AIA/NDIA FALL CONFERENCE

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

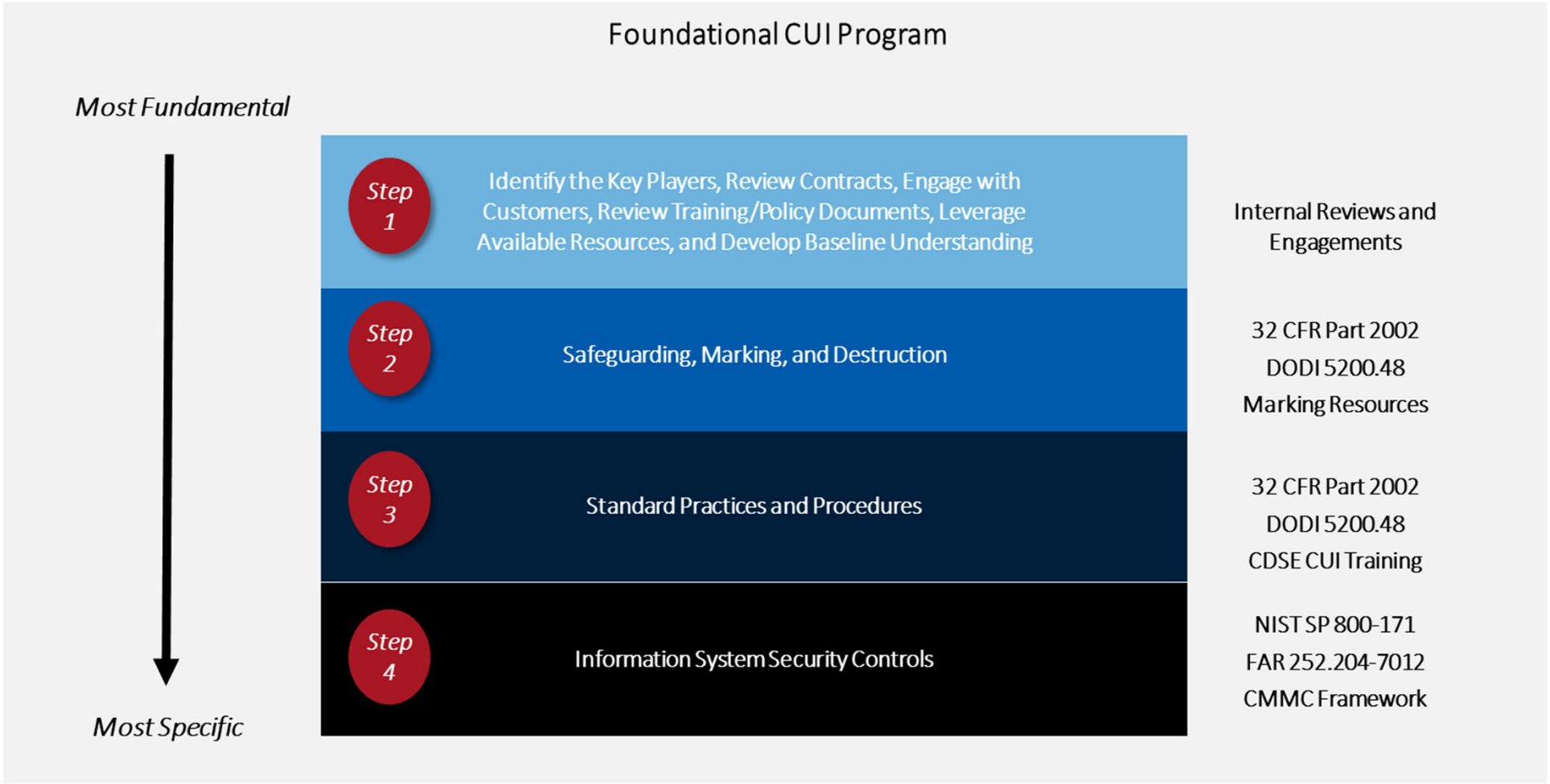
John B. Massey
Deputy Assistant Director
Enterprise Security Operations
DCSA Critical Technology Protection

APPROVED FOR PUBLIC RELEASE

Agenda

- Building the Foundation
- The Key Players
- Training and Policy Documents
- Contract Review and Customer Engagement
- Leverage Available Resources
- Standard Practices and Procedures
- Safeguarding and Destruction
- Information System Security Controls and CMMC Familiarization

Building the Foundation



The Key Players

Who are the key players in your organization's security program?

- Facility Security Officer
- Senior Management
- Insider Threat Program Senior Official
- Information Systems Security Manager
- Program Managers
- Engineers
- Contracting and Acquisition Professionals

Does your facility need a dedicated CUI Manager?

How do you educate them in CUI?

- One-Pagers
- Share DCSA resources
- Incorporate into training
- Host a brown bag luncheon
- Introduce them to the CUI Registry
- Share CDSE training course

Training and Policy Documents

Training

- DOD Mandatory CUI Training – when requested by the Government Contracting Activity when contracts contain CUI requirements
- Required annually (DOD)

Policy Documents

- EO 13556
- 32 CFR Part 2002
- NIST SP 800-171
- FAR 252.204-7012
- DoDI 5200.48

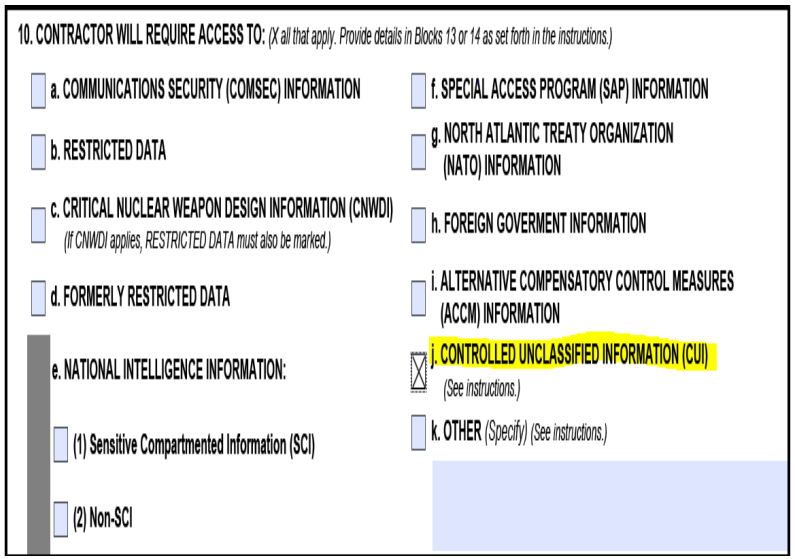
Registry Information

- National CUI Registry
- DOD CUI Registry
  - Registries support familiarization with types of information that may be CUI.
  - Registries are used by Government Contracting Activities to determine what is CUI.

Contract Review and Customer Engagement

Contract Review

- DD Form 254
  - Look for the CUI indicator in BLOCK (10 j.).
  - Look within BLOCK (13) for additional information on security requirements.
- Search other contract documents that may indicate access to CUI is required.
- If found in other documents and not listed in the DD Form 254, contact the GCA to facilitate discussion on reissuing an updated DD Form 254.
- If you believe a contract includes access to CUI but CUI requirements are not found in contractual documents (RFQ, RFP, DD 254, etc.), consult your GCA.



10. CONTRACTOR WILL REQUIRE ACCESS TO: *(X all that apply. Provide details in Blocks 13 or 14 as set forth in the instructions.)*

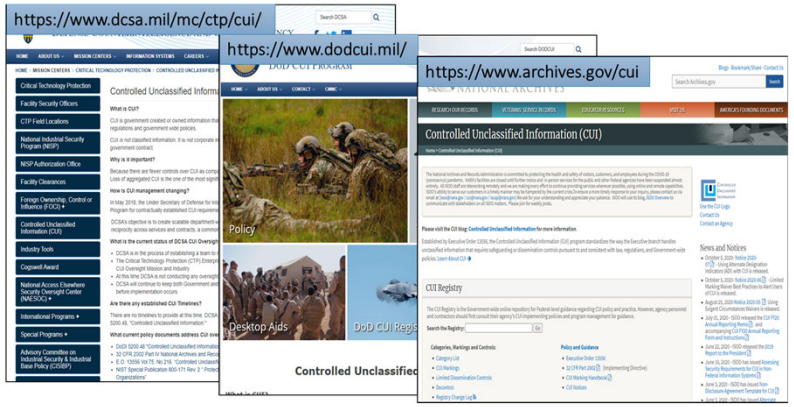
☐ a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	☐ f. SPECIAL ACCESS PROGRAM (SAP) INFORMATION
☐ b. RESTRICTED DATA	☐ g. NORTH ATLANTIC TREATY ORGANIZATION (NATO) INFORMATION
☐ c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI) *(If CNWDI applies, RESTRICTED DATA must also be marked.)*	☐ h. FOREIGN GOVERMENT INFORMATION
☐ d. FORMERLY RESTRICTED DATA	☐ i. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM) INFORMATION
☐ e. NATIONAL INTELLIGENCE INFORMATION:	☒ j. CONTROLLED UNCLASSIFIED INFORMATION (CUI) *(See instructions.)*
☐ (1) Sensitive Compartmented Information (SCI)	☐ k. OTHER *(Specify) (See instructions.)*
☐ (2) Non-SCI	

Note: *You will likely find that each individual GCA is at a different place with implementing their CUI program and incorporating CUI requirements into contracts.*

Leverage Available Resources

Resources are available!

- DoD CUI Website: www.dodcui.mil
- NARA Website: www.archives.gov
- CDSE CUI Toolkit: www.cdse.edu
- DCSA Website: www.dcsa.mil/mc/ctp/cui/



DCSA Website Resources

- CUI Slick Sheet
- CUI FAQ
- CUI Quick Start Guide
- DCSA and DoD CUI Marking Job Aids
- NARA CUI Marking Handbook
- CUI Quick Reference Guide
- CUI Cover Sheet

- Disseminate resources to key players and have them readily available

Standard Practices and Procedures

Consider an SPP. But what would one look like?

If you have no or minimal CUI requirements…

- Baseline information and overview of CUI Program

If you have a moderate number of contracts with CUI requirements…

- Baseline information and overview of CUI Program
- Facility specific procedures
- Educational and training resources

If you a significant number of contracts with CUI requirements…

- Baseline information and overview of CUI Program
- Facility specific procedures
- Educational and training resources
- Contract-specific guidance

Safeguarding and Destruction

Safeguarding

- Follow requirements outlined in contract documentation (Block 13 - DD 254).
- To ensure CUI protection, the following measures will be implemented:
  - During working hours, steps will be taken to ***minimize the risk of access by unauthorized personnel***, such as not reading, discussing, or leaving CUI information unattended where unauthorized personnel are present.
  - After working hours, CUI information will be ***stored in unlocked containers, desks, or cabinets*** if the government or government-contract building provides security for continuous monitoring of access. If building security is not provided, the information will be ***stored in locked desks, file cabinets, bookcases, locked rooms, or similarly secured areas***.

Destruction

- CUI in all formats (hard copy, electronic, in media, etc.) will be destroyed when it is deemed to no longer to meet the threshold to be considered CUI and there are no safeguarding measures required.
- Record and non-record CUI documents may be destroyed by means approved for destroying classified information or by any other means making it unreadable, indecipherable, and irrecoverable.

Marking CUI

Leverage job aids and make them readily available to personnel actively working with CUI

Safeguarding and Destruction

Create: CUI is created when put on paper or entered into an information system.

Identify & Designate: Realize that the information is generated for or on behalf of an agency within the Executive Branch under a contract and determine if the information falls into one of the more than one hundred categories of CUI in the National CUI Registry. It is also important to realize what is not CUI.

Mark/Label: At minimum, CUI markings for unclassified DOD documents will include the acronym "CUI" or "CONTROLLED" in the banner of the document. It is a best practice to include markings in both the banner and footer of the document, and it is imperative to reference the CUI Marking Guide to ensure correct markings.

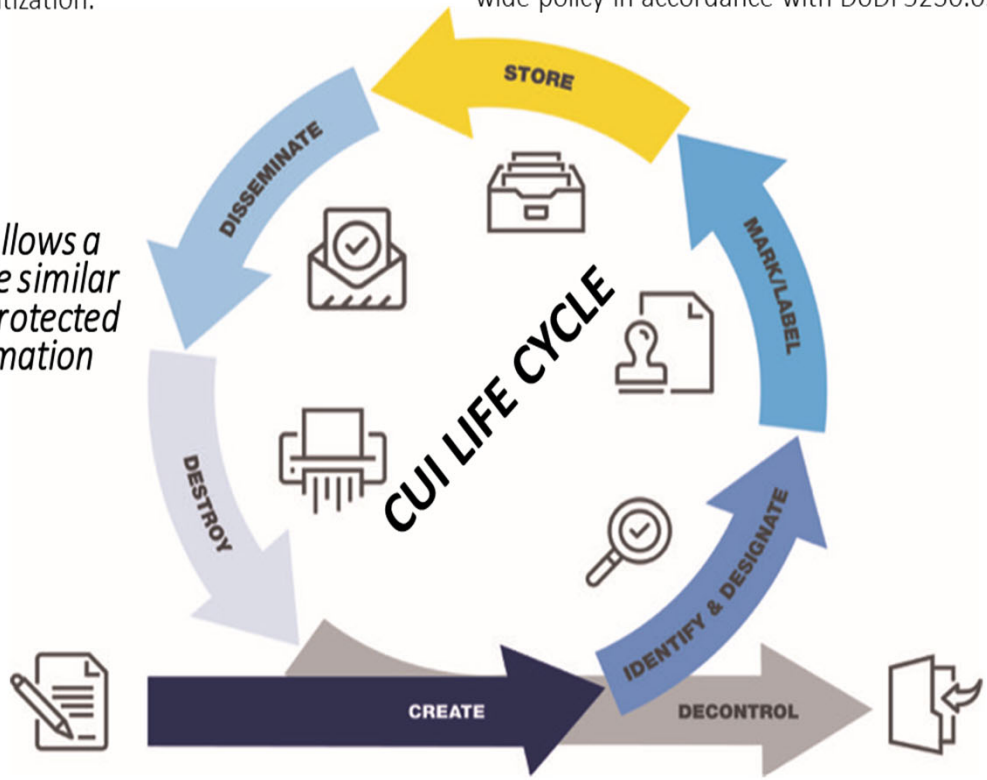
Store: CUI can be stored in NIST SP 800-171 compliant information systems or controlled physical environments.

Disseminate: Only authorized holders may disseminate in accordance with distribution statements, dissemination controls, and applicable laws.

Destroy: Hard and soft copies of CUI should be appropriately destroyed, meaning they are rendered unreadable, indecipherable, and irrecoverable. Review clearing, purging, and destruction in NIST SP 800-88: Guidelines for Media Sanitization.

Decontrol: Agencies must promptly decontrol CUI once the CUI owner has properly determined the information no longer requires safeguarding or dissemination controls, unless doing so conflicts with the related law, regulation, or government-wide policy in accordance with DoDI 5230.09.

CUI follows a lifecycle similar to all protected information



Information Security Controls / CMMC Familiarization

Information System Security Controls

- Become familiar with NIST SP 800-171, Rev 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.
- A security controls job aid is currently under development and will support implementation of 110 NIST SP 800-171 security controls.

Cyber Maturity Model Certification (CMMC)

- Become familiar with CMMC.
- CMMC stands for “Cybersecurity Maturity Model Certification” and is a unifying standard for the implementation of cybersecurity across the Defense Industrial Base (DIB).
- The CMMC framework includes a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level.
- CMMC is designed to provide increased assurance to the Department that a DIB company can adequately protect sensitive unclassified information, accounting for information flow down to subcontractors in a multi-tier supply chain.
- Review the CMMC FAQs: www.acq.osd.mil/cmmc/faq.html

Questions?

DEFENSE
COUNTERINTELLIGENCE
AND SECURITY AGENCY