



NISPPAC Security Policy Updates



Heather M. Sims
General Dynamics
Industrial Security Strategy
hsims@gd.com

industry nisppac@gmail.com

Updated: 10/1619



NISPPAC Members

GOVERNMENT

Mark Bradley, Chair	ISOO
Michael Mahoney	CIA
Keith Minard/Karl Hellmann	*DCSA
Sharon Donglinger	*Air Force
James Anderson	Army
Richard Townsend	Commerce
Heather McMahon	DOD
Marc Brooks	Energy
Steven Lynch	DHS
Christine Gunning	DOJ
Dr. Mark Livingston	Navy
Kimberly Baugher	DOS
Zudayyah L. Taylor-Dunn	NASA
Amy Davis	NSA
Denis Brady	NRC
Valerie Kerben	ODNI

INDUSTRY

Heather Sims, Spokesperson	*General Dynamics
Aprille Abbott	*MITRE
Rosie Borrero	ENSCO
Brian Mackey	BAE Systems
Dan McGarvey	Alion S & T
Dennis Arriaga	SRI International
Bob Harney	Northrop Grumman
Cheryl Stone	RAND Corp.

Jessica Giguere,
Industry
Coordinator *

BAE

Katie Timmons,
Industry
Coordinator*

ViaSat

MOU

Kai Hanson	AIA
Matt Hollandsworth	ASIS
Joe Kraus	CSSWG
Shawn Daley	FFRDC/UARC
Kathy Pherson	INSA
Marc Ryan	ISWG
Cathe Kaohi	NCMS
Rick Lawhorn	NDIA
Charles Sowell	PSC



PICK A TOPIC, ANY TOPIC

**NEW
ISLs**

CMMC

**DCSA
ORG**

SEADS

**E-MASS,
NCCS,
DISS&NISS**

NAESOC

CUI

**CLEARANCE
TIMELINES**

**STUMP THE
CHUMPS**



NISPPAC 101

- **ESTABLISHMENT:** The NISPPAC was created on January 8, 1993, by the President under Section 103 of **Executive Order 12829, "NISP"**
Functions: The NISPPAC members **advise the Chair of the Committee on all matters concerning the policies of the NISP**, including **recommending changes** to those policies as reflected in the Order, its implementing directives, or the operating manual established under the Order, and serves as a **forum to discuss policy issues in dispute.**



NISPPAC Working Groups

- Policy-NEW Replacing the NISPOM Re-Write
- NID
- Clearance
- Insider Threat
- Risk-based Security Oversight (RISO)-Formally DiT
- NISA
- NCCS-NEW



National Level Policy

- NISPOM Rewrite
- Conforming Change 3
- CUI Note: 2019-XX-Assessing Security Requirements for CUI within Non-Federal Information Systems
- Draft ISLs
 - ✓ Investments in Marijuana
 - ✓ Usage of EPL List and Crosscut Shredders
 - ✓ SEAD 3-Adverse Information Reporting
 - ✓ Tailored Security Plan
 - ✓ Top Secret Accountability (pending release for review)





Trusted Workforce 2.0: Industry Observations

- **Policy delays**

- National Security Policy Memo (NSPM) to be signed by the President.
- SEC/EAs releasing Executive Correspondence (EC) after the NSPM that will:
 - Initiate an improved investigative process, paving the way for the new vetting policy to follow

- **New policy**

- ODNI Guidance for Reciprocal Acceptance of Deferred Periodic Reinvestigations (29 Sep19)
 - Not publicly available to industry due to FOUO marking

- **Industry Concerns**

- Policy timelines
- Transition from Reciprocity to Transfer of Trust
- Transition of Continuous Evaluation to Continuous Vetting



Security Executive Agent Directives (SEADs)

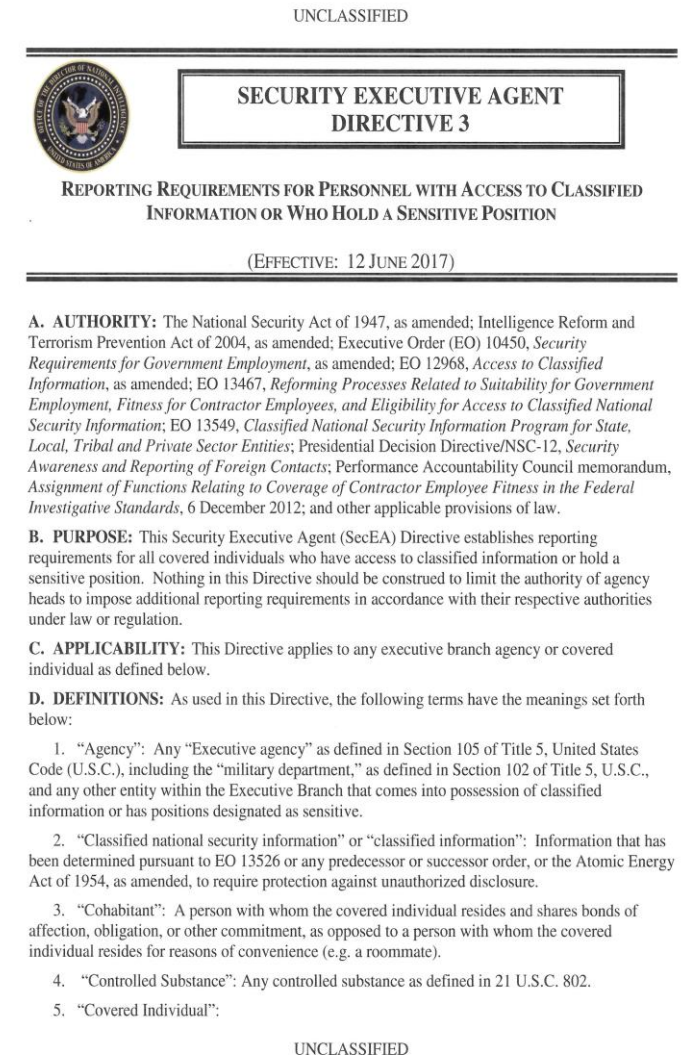
- SEAD 1: SECEA Authorities and Responsibilities
- SEAD 2: Use of Polygraphs
- SEAD 3: Reporting Requirements for Personnel with Access to Classified
- SEAD 4: National Security Adjudicative Guidelines
- SEAD 5: Social Media usage in Investigations and Adjudications
- SEAD 6: Continuous Evaluation
- SEAD 7: Reciprocity
- SEAD 8: Interim Clearances (IN DRAFT)

All SEADs can be found here: <https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-policy>



SEAD 3: Minimum Reporting Requirements


- Signed December 14, 2016 – Implementation June 12, 2017.
- All covered persons are to report “CI Concerns” on any other covered person. Previously was limited to only those within an organization. Change raises possible legal and other concerns.
- “Failure to comply with reporting requirements...may result in administrative action that includes, but is not limited to revocation of national security eligibility.”
- Pre-approval for foreign travel will be required for collateral clearance holders once it is incorporated into the new NISPOM. This will impose a new and large burden on industry and CSAs to handle the influx of reports that this will now generate. (ISL will not require pre-approval but will require tracking and reporting).
- [DNI SEAD 3 TOOLKIT is online.](#)
- Collateral under the NISP will not have to comply until incorporated into NISPOM Conforming Change 3 and resulting ISL.
- Draft ISL outlines FSO in collaboration with ITPSO responsible for tracking and monitoring all foreign travel for “covered” personnel
- Other CSAs will issue their own implementation guidance.





SEAD 6: Continuous Evaluation

- SEAD 6: Continuous Evaluation signed January 12, 2018
- 1.1 Million now enrolled in CE
- OUSD(I) Memo dated 12/19/2016: DSS will be responsible for the CE mission.
- DSS actively enrolling both government and industry in CE.
- CE dates will be put in DISS, but not JPAS. Historical CE dates will be included dating back to 2012.
- CE replacing PRs is still an interim process and could be subject to change.
- If your customer requires an investigation instead of CE, please email dss.ncr.dss-isfo.mbx.psmoi@mail.mil for assistance.

 UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

DEC 19 2016

MEMORANDUM FOR DIRECTOR, DEFENSE SECURITY SERVICE
CHIEF OF STAFF, OFFICE OF THE UNDER SECRETARY OF
DEFENSE FOR INTELLIGENCE
DIRECTOR FOR DEFENSE INTELLIGENCE, INTELLIGENCE
STRATEGY, PROGRAMS & RESOURCES, OFFICE OF THE
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
DIRECTOR, COUNTERINTELLIGENCE & SECURITY,
OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR
INTELLIGENCE

SUBJECT: Realignment of the Department of Defense Continuous Evaluation Mission and
Resources to the Defense Security Service

I hereby realign the Department of Defense (DOD) and CE Validation Cell resources from the Security
Defense Security Service (DSS). Upon this realign-
ment, the DSS Personnel Security Management Office (PSMO) will
prepare the Department to meet its goal of implementing
the end of calendar year 2017.


The Security Policy and Oversight Division (SPOD) will
CE Program of Record. Additionally, SPOD will
associated responsibilities, functions, relationships.

DSS will provide quarterly progress updates
In accordance with the Office of the Secretary of Defense
Secretary of Defense for Intelligence will retain all

Mare

cc:
Director for Defense Intelligence (Intelligence & Security)

UNCLASSIFIED

 **SECURITY EXECUTIVE AGENT
DIRECTIVE 6**

CONTINUOUS EVALUATION
(EFFECTIVE: 12 JANUARY 2018)

A. AUTHORITY: The National Security Act of 1947, as amended; Intelligence Reform and
Terrorism Prevention Act of 2004, as amended; Security Clearance Information Act, as
amended; Executive Order (EO) 12968, *Access to Classified Information*, as amended; EO
13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for
Contractor Employees, and Eligibility for Access to Classified National Security Information*, as
amended; EO 13549, *Classified National Security Information Program for State, Local, Tribal
and Private Sector Entities*, and other applicable provisions of law.

B. PURPOSE: This Security Executive Agent (SecEA) Directive establishes policy and
requirements for the continuous evaluation (CE) of covered individuals who require continued
eligibility for access to classified information or eligibility to hold a sensitive position.

C. APPLICABILITY: This Directive applies to any executive branch agency, authorized
adjudicative agency, authorized investigative agency, and covered individuals as defined below.

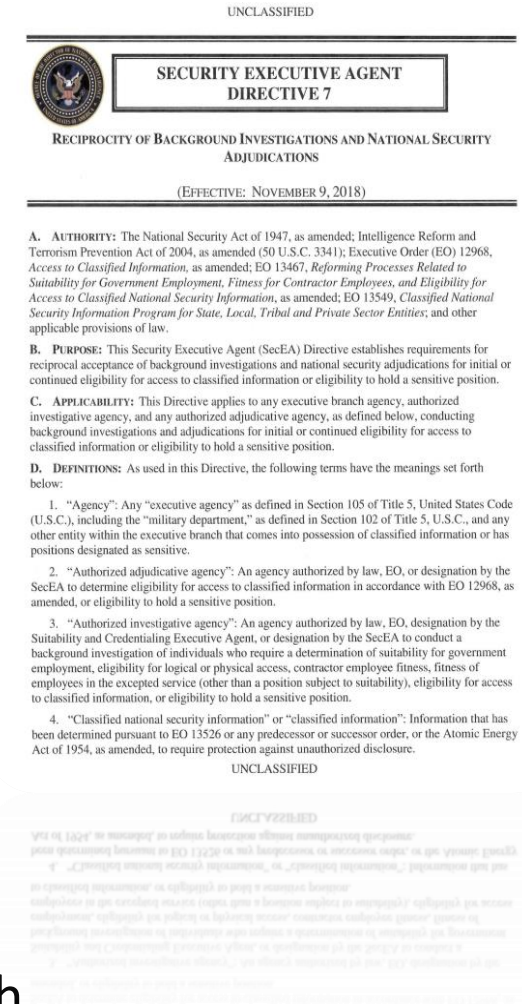
D. DEFINITIONS: As used in this Directive, the following terms have the meanings set forth
below:

1. "Agency": Any "executive agency" as defined in Section 105 of Title 5, United States
Code (U.S.C.), including the "military departments," as defined in Section 102 of Title 5, U.S.C.,
and any other entity within the executive branch that comes into possession of classified
information or has positions designated as sensitive.
2. "Authorized adjudicative agency": An agency authorized by law, executive order, or
designation by the SecEA to determine eligibility for access to classified information in
accordance with EO 12968, as amended, or eligibility to hold a sensitive position.
3. "Authorized investigative agency": An agency authorized by law, executive order, or
designation by the SecEA to conduct a background investigation of individuals who are
proposed for access to classified information or eligibility to hold a sensitive position or to
ascertain whether such individuals continue to satisfy the criteria for retaining access to such
information or eligibility to hold such positions.
4. "Classified national security information" or "classified information": Information that
has been determined, pursuant to EO 13526, any predecessor or successor order, or the Atomic
Energy Act of 1954, as amended, to require protection against unauthorized disclosure.



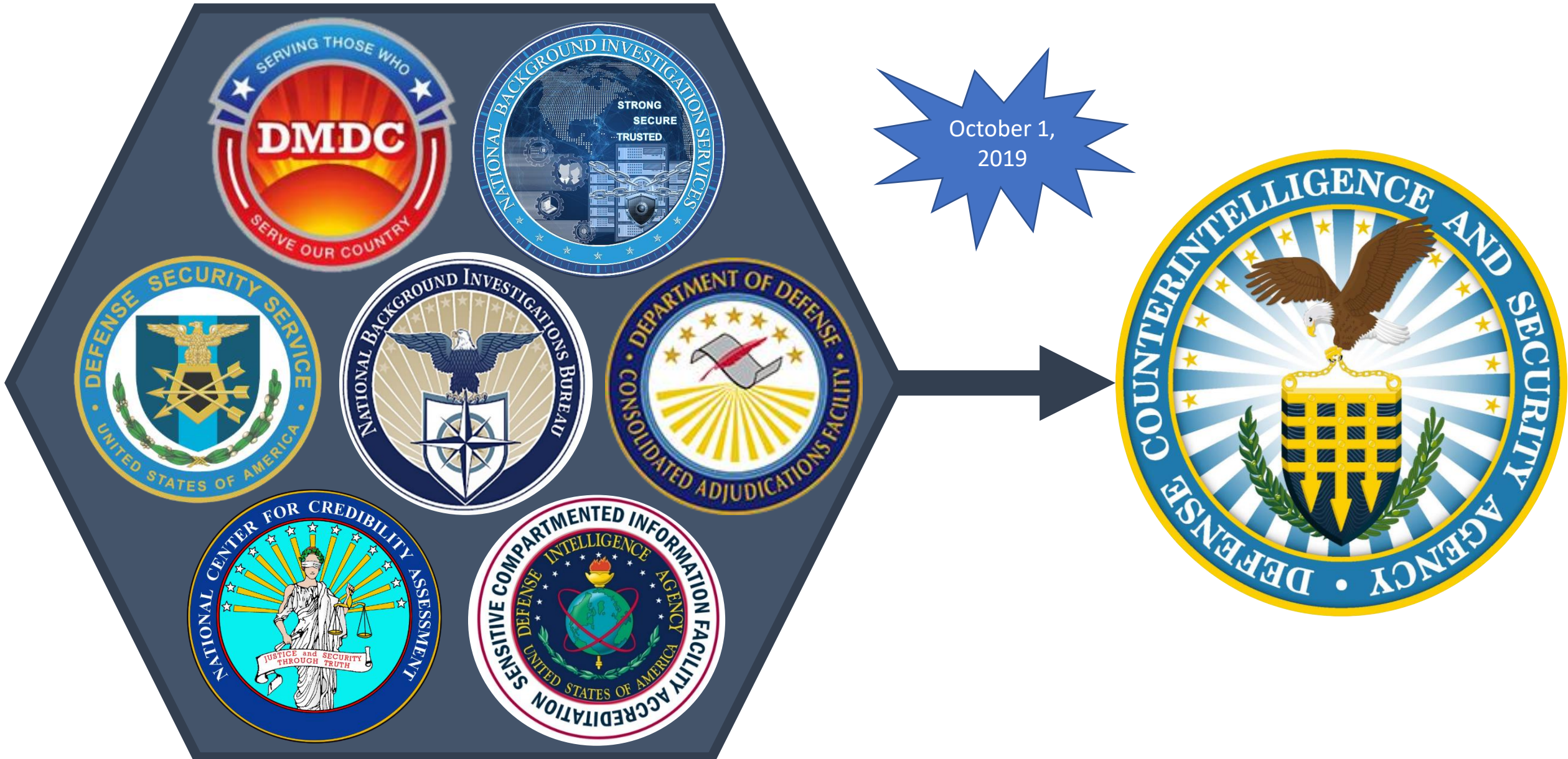
SEAD 7: Reciprocity

- “Background investigations...conducted by an authorized investigative agency...shall be reciprocally accepted for all covered individuals except...[if] the most recent background investigation is more than seven years **old unless otherwise directed by the SecEA...While not required, agencies may accept background investigations more than seven years old on a case-by-case basis.**”
 - *This wording may cause challenges for cases enrolled in CE that will not have an investigation date within 7 years.*
- Timelines:
 - “**Reciprocity determinations** for national security background investigations and adjudications **shall be made within five business days** of receipt by the agency's personnel security program for security processing.”
 - “Agencies in possession of the investigative record shall comply with requests for the investigative record within 10 business days.”





DCSA: Defense Counterintelligence and Security Agency





VROC Metrics as of 9/24/2019

Industry e-QIP & Interim Determination Metrics

FY 19 e-QIP Submissions **101,529**

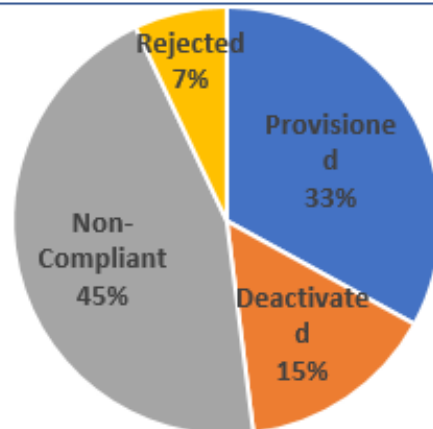
Current e-QIP Inventory **17,086**

FY19 PRs deferred to CE **36,586**

FY 19 Interims Processed **72,539**

Interim Timeliness **Average 15 days**

DISS Provisioning Status



DoD Continuous Vetting

CE Population Jun 2019

1,346,890

CE Alerts Received

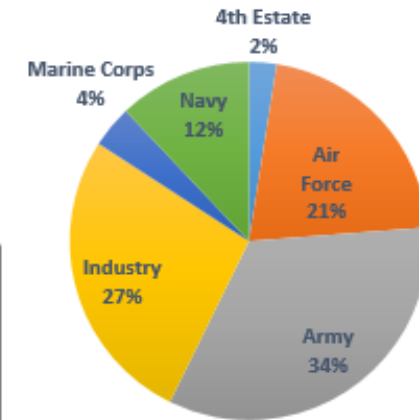
FY17 - 26,843
FY18 - 47,453
81,260

Early Detection

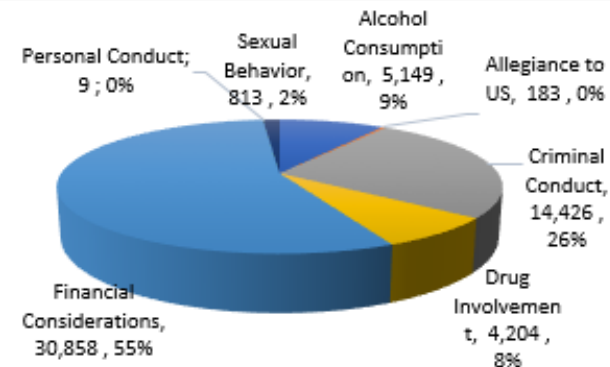
Secret: 6yr 7mo
TS: 2yr 5mo

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

Population By Department



CE FY19 Alerts by Guideline





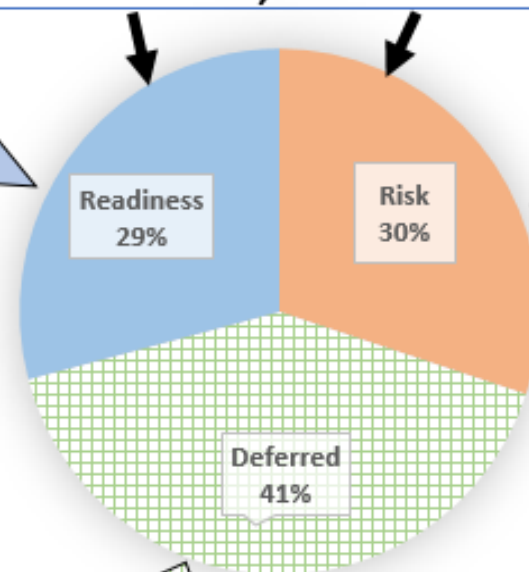
DOD CAF

Readiness Portfolio

- T1/T3/T5 Initials (22 days)
- Expedites
- Interim SCI
- Key Management Personnel (KMP)
- Reciprocity
- Recertify/Reconsideration/Upgrade

Industry Work-in-Progress

36,533



Risk Management Portfolio

- T3R/T5R Medium/High Risk
- CE Alerts
- Incident Reports
- REO/RSI
- Supplemental Information

Strategic Priorities

1. Aging inventory reduction
2. Inventory size reduction
3. Improve quality and consistency of decision making & business processes

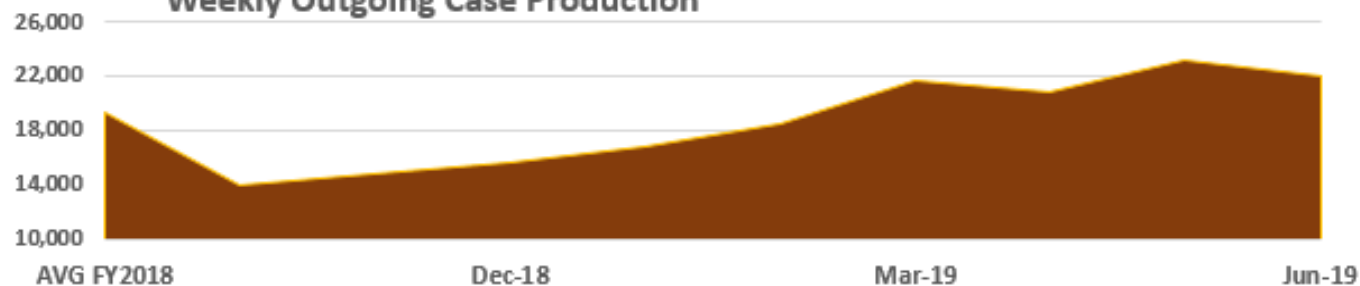
Deferred PR Adjudications Portfolio

- T3R/T5R Low to No Risk

Efficiency Initiatives

- ✓ Lean Six Sigma
- ✓ Reorganization
- ✓ "All Hands on Deck"
- ✓ Targeted inventory reductions
- ✓ Deferred PR adjudications
- ✓ Increased workforce flexibility
- ✓ Robust use of OT
- ✓ Reciprocity

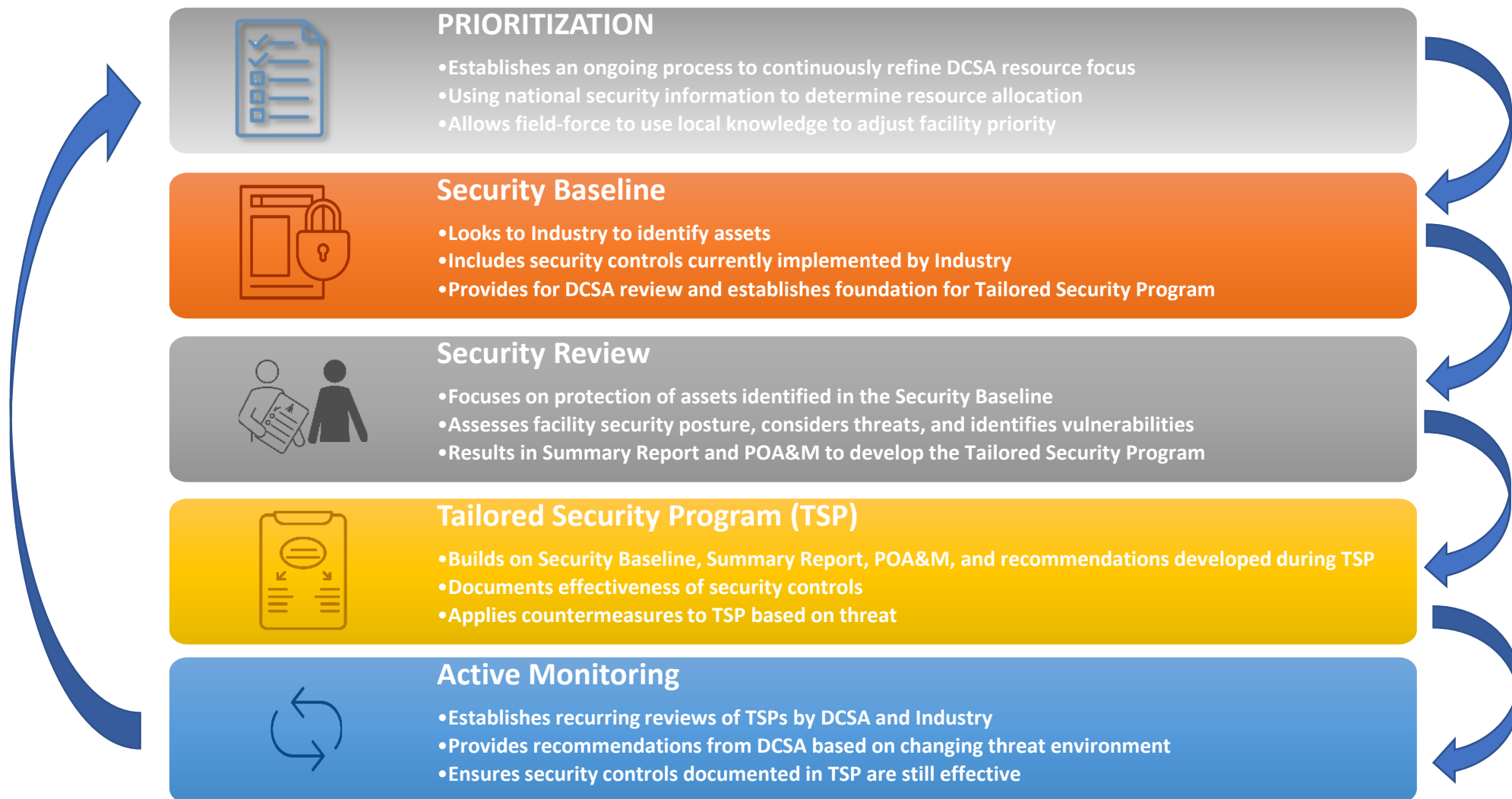
Weekly Outgoing Case Production





Risk-Based Industrial Security Oversight (RISO)

(Formerly DCSA in Transition)





Ongoing Business: RISO

Industry Questions / Concerns

- Very little engagement between DCSA and RISO/DiT Industry Focus Group over the past 7 months
 - March informational meeting on Security Rating Score
 - July telecon on RISO status
- Variances in implementation between DCSA field offices and inconsistencies within DCSA activities on RISO (Engagement Terminology)
- Industry adoption of elevated Industrial Security Requirements Tailored Security Plan (TSP's)
- Smaller companies without key technologies will not be assessed and the vulnerabilities this might introduce into the supply chain
- Coordination w/ GCA's and the concern about the impacts of introducing vulnerability information to the GCA outside the contract scope

Industry Proposed Solutions/Requests

- Industry requests the opportunity for collaboration when coordinating with the GCA's on vulnerability information
- Reengage DCSA/RISO Industry Focus group partnership and collaboration. What is the status of the Security Rating Score to Replace Enhancement Matrix

Activity	Asset ID	Business Processes	12x13	TSP	Rating
Comprehensive Security Review	Yes	Yes	Yes	Yes	No
Targeted Security Reviews	Yes	Yes	Yes	No	Yes
Enhanced SVAs	Introduce	Introduce	Introduce	No	Yes
Meaningful Engagements	No	No	No	No	No



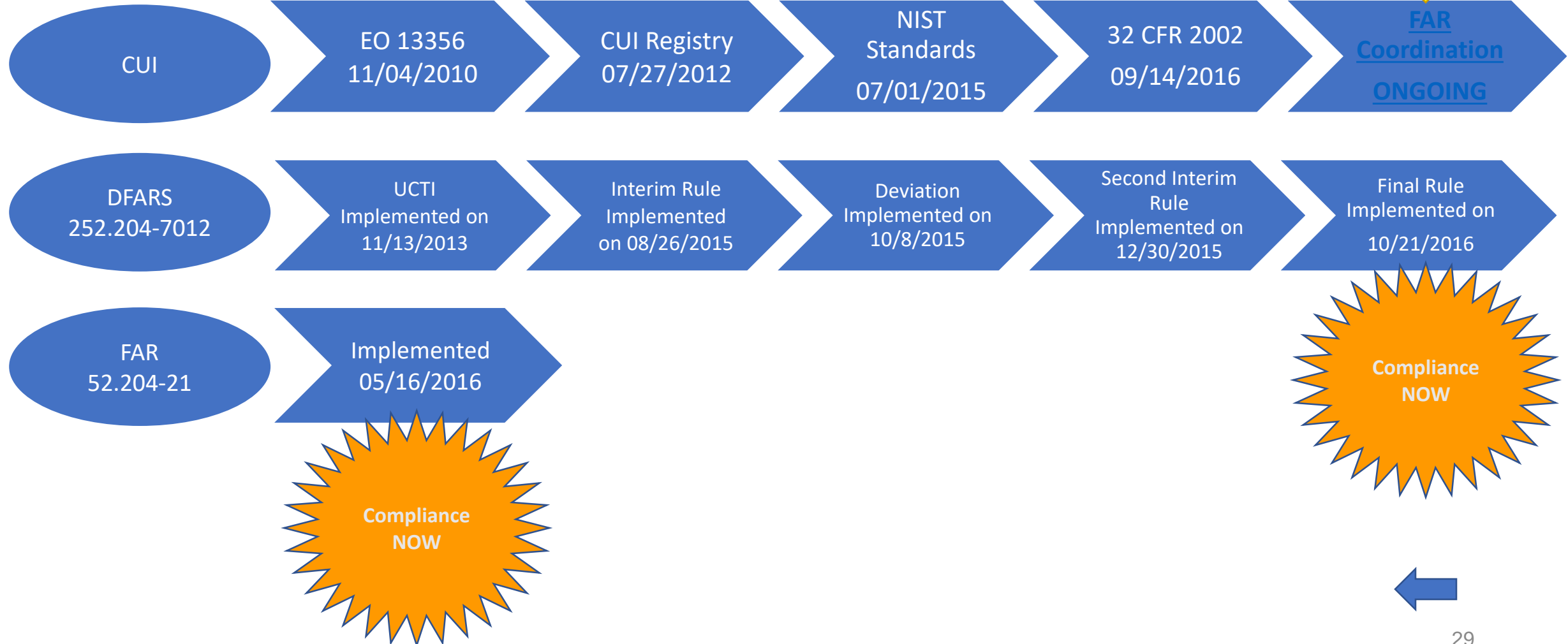
NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

- 500 facilities from across the United States have been selected to participate, but the number will grow to 2,000 by October 2019.
- A variation of the traditional DCSA Field Office, specifically designed to support non-possessing facilities regardless of their physical location.
- This consolidated and centralized approach to non-possessor facilities provides the DCSA Director with a flexible and efficient method for addressing industry compliance issues.
- The NAESOC will be a centralized resource for both government and industry partners providing communications and oversight for non-possessor requirements and issues.





CUI/CDI/Federal Contract Information





Cybersecurity Maturity Model Certification (CMMC)

- January 2020, DoD will be implementing CMMC across industry. companies will be required to achieve a CMMC level of 1-5 in order to perform work on DOD initiatives.
- Small businesses should be able to easily achieve a CMMC level of 1.
- The CMMC model will be agile enough to adapt to emerging and evolving cyber threats to the DIB sector. A neutral 3rd party will maintain the standard for the Department.
- The CMMC will include a center for cybersecurity education and training.

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





Policy Changes and Impacts on our Radar

Industry Questions / Concerns

- New proposed Facility Pre-decisional Security Rating Score (SRS)
- Continuous Evaluation (CE) and lack of understanding concerning terminated employees
- Agencies not recognizing reciprocity of individuals in CE that are out of scope
- Deferring of closed investigations pending adjudication at the DOD CAF and what deferred means
 - Impact to reporting requirements for timeliness of adjudications
- Future OUSDI guidance on use of marijuana, ownership of stocks involved with marijuana and use of other products derived from marijuana (marijuana/CBD oil purchased for your pet) – is this reportable?
- NSA released new Evaluated Products List (EPL) and removed equipment that had been previously approved for DVD destruction. Industry was left in limbo with no guidance from sponsoring agencies.
 - Draft ISL received for review concerning guidance from DCSA when an EPL is updated, awaiting feedback on comments
- Accounting for Top Secret material when in electronic form
- DMDC JPAS report feeds into other systems
- Too much all at once-new systems, new ISL, CMMC, RISO, CUI, Delivering Uncompromised

Industry Proposed Solutions / Requests

Implementation is difficult when Industry expertise is not leveraged early in the planning process. Collaborating with Industry will reduce some of the challenges when executing new national security policy.



Industry NISPPAC on the Web

<https://classmgmt.com/nisppac.php>



NATIONAL INDUSTRIAL SECURITY PROGRAM
POLICY ADVISORY COMMITTEE (NISPPAC)

HOME

Login

Join NCMS

About



Chapters



Events



► Industry NISPPAC

NCMS Speaker Database

Scholarship Program

Member Résumés

Contact

NATIONAL INDUSTRIAL SECURITY PROGRAM POLICY ADVISORY COMMITTEE (NISPPAC)

Industry Representatives' Informational Site

About

NISPPAC Industry
Members

MOU
Group

Working
Groups

News &
Resources

Policy
Timeline

Official
Website

In April 1990, President George Bush directed the National Security Council to explore the creation of a single, integrated industrial security program that might result in cost savings and improved security protection.

Recommendations from representatives from government and industry were invited to participate in an initiative intended to create an integrated security framework. This initiative led to the creation of Executive Order (EO) 12829, which established the National Industrial Security Program (NISP), a single, integrated, cohesive security program to protect classified information and to preserve our Nation's economic and technological interests.

EO 12829 also established the National Industrial Security Program Policy Advisory Committee (NISPPAC). The NISPPAC is chaired by the Director of the Information Security Oversight Office (ISOO), who has the authority to appoint sixteen representatives from Executive Branch agencies and eight non-governmental members. The eight non-governmental members represent the approximately 13,000 cleared defense contractor organizations and serve four year terms.

This website serves as a way for industry to gain a better understanding of the non-governmental members involvement in order to help the community stay abreast of the ever-changing security posture.

To watch a short video on the history of the NISP, [click here](#)

[Charter](#)  | [Bylaws](#)  | [Upcoming Public NISPPAC meeting](#)

Contact

Member Résumés

NCMS Speaker Database

[Charter](#)  | [Bylaws](#)  | [Upcoming Public NISPPAC meeting](#)

To watch a short video on the history of the NISP, [click here](#)



Where do we go from here?

- **Industry engagement at all levels and often**
- **Identify issues quickly with solutions**
- **Industry unity in how we communicate to the government**
- **What are the Top 5-10 Industry Issues?**
- **Don't suffer in silence-Bring Issues forward**
- **BESIDES THAT, HOW ARE THINGS GOING?**