MARCH 2016

DOD Insider Threat Management and Analysis Center

COUNTERINTELLIGENCE AWARENESS WEBINAR SERIES

DITMAC

Host: Rebecca Morgan Insider Threat Instructor - CDSE

Guests:

- **Matt Guy** – Asst. Director, Program Evaluation
- **Delice Bernhard** – Asst. Director, Operations
- **Mark Burns** – Asst. Director, Strategic Integration

Navigation in the Meeting Room

Enlarge Screen

Q & A

File Share

DOD INSIDER THREAT MANAGEMENT AND ANALYSIS CENTER

DITMAC

March 7, 2016

Today's Agenda

AGENDA

- DITMAC mission and status
- Defining *insider threat*
- Analyzing behavior
- Supporting DoD and its 43 Components
- Q&A

The Challenge

"One person can compromise information that can cripple our government. One person can expose the strategies that keep America safe. One person can walk into a workplace with a weapon and commit an atrocity. The insider threat is insidious. It's hiding among the people we trust most."

-- Hon. James R. Clapper, Director of National Intelligence

Remarks at National Insider Threat Task Force Legal Forum, October 28, 2015

What is an Insider Threat?

INSIDER:

"Any person with authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD."

INSIDER THREAT:

"The threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities."

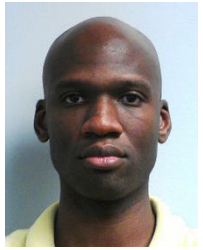
DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014

High Profile Examples

November 5, 2009 – Army Major Nidal Hasan fatally shoots 13 and injures 30 others at Fort Hood, TX

May 27, 2010 – Army Private Bradley Manning Arrested for illegally disclosing 1,000,000+ classified documents

June 9, 2013 – Cleared Contractor Edward Snowden identifies himself as leaker of Top Secret NSA information



September 16, 2013 – Cleared Contractor Aaron Alexis fatally shoots 12 and injures 3 others at the Washington Navy Yard

DoD Insider Threat (InT) Programs

November 12, 2012 Presidential Memorandum set requirements for Executive Branch InT Programs, including **DoD and DoD Components**

1. **Designate a Senior Official responsible the InT Program**
2. **Obtain Visible Support from the Agency Head**
3. **Form a Working Group/Periodic feedback to the Community**
4. **Review Current Requirements and Guidance**
5. **Seek Legal Input**
6. **Protect Privacy and Civil Liberties by Applying Appropriate Safeguards**
7. **Identify Classified and other Critical Assets**
8. **Write Agency Policy and Implementation Plan**
9. **Obtain approval, Establish Program Office, Implement Plan**
10. **Conduct scheduled self assessments**

DITMAC Background

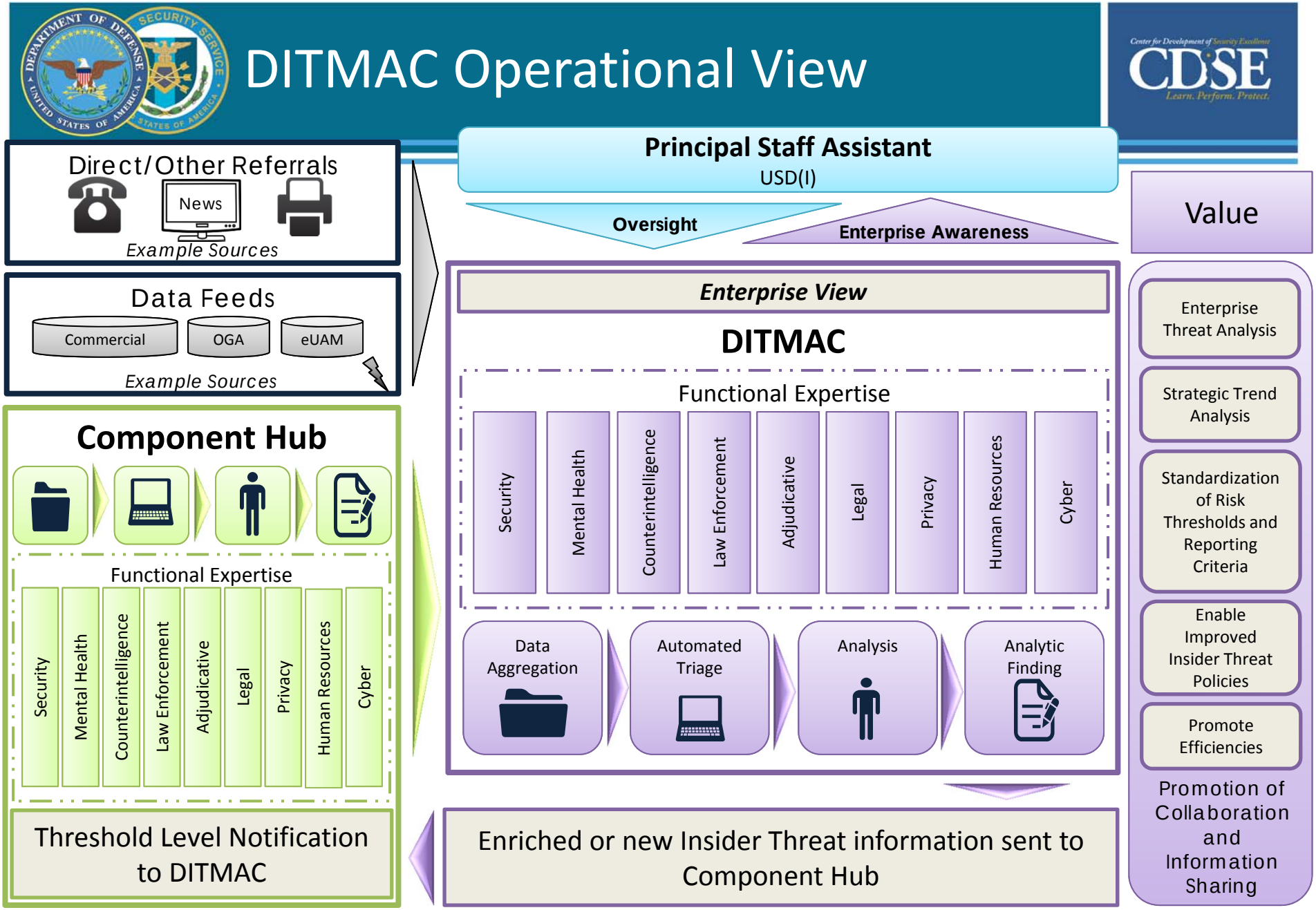
DITMAC: DoD Insider Threat Management and Analysis Center

USD(I) assigned the DITMAC incubation mission to the Defense Security Service (DSS) in December 2014

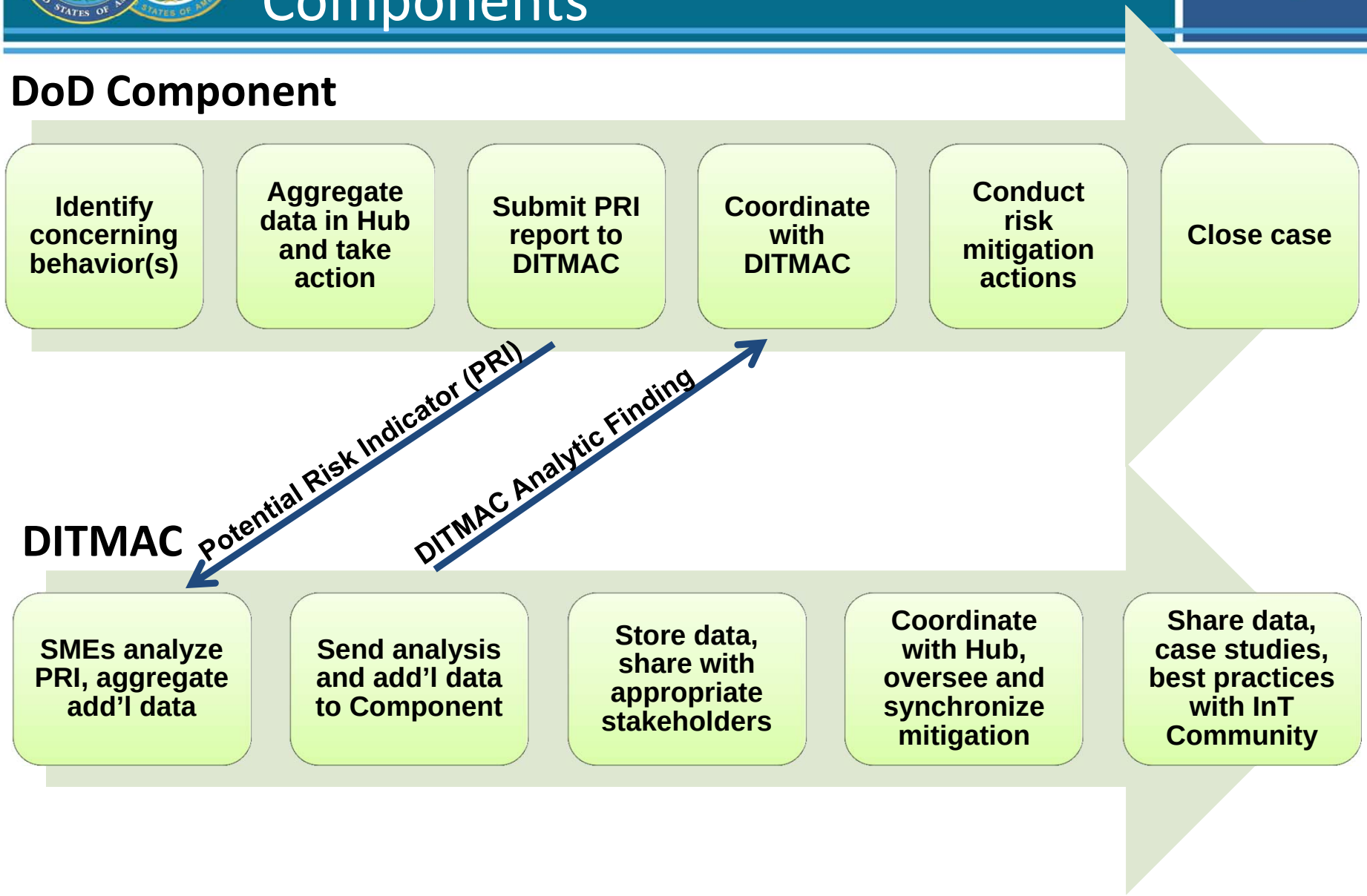
<u>An enterprise insider threat capability for DoD to:</u>

- Oversee the mitigation of insider threats to DoD
- Assess risk, refer recommendations for action, synchronize responses, and oversee resolution of identified issues
- Develop risk thresholds and compile results for evaluation
- Ensure DoD InT Programs remain compliant to applicable regulations, including the National InT minimum standards
- Provide a single repository for DoD insider threat related information
- Promote collaboration and information sharing

DITMAC Operational View

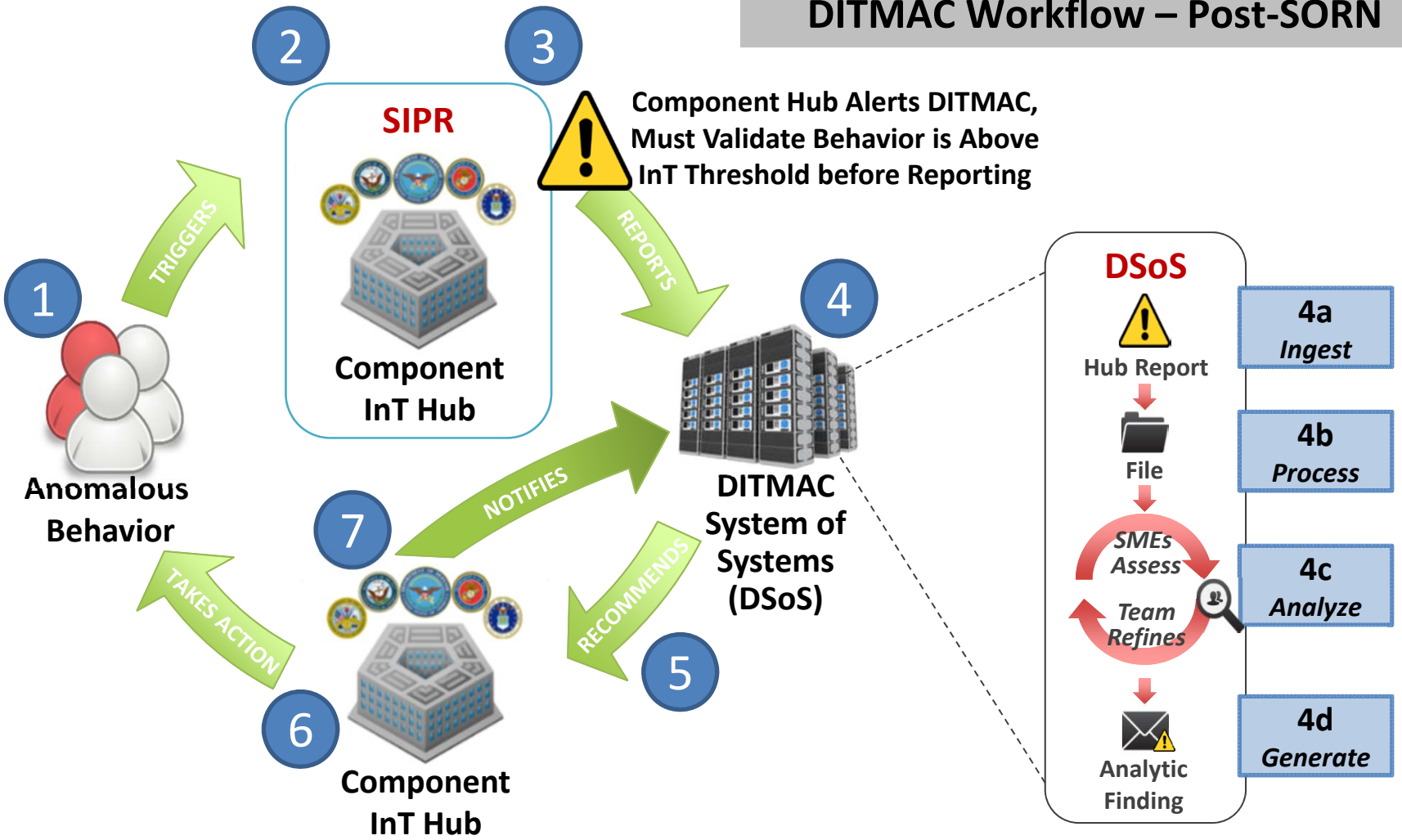


DITMAC Support to DoD Components



DITMAC System of Systems (DSoS)

DITMAC Workflow – Post-SORN



PIOC Component Reporting

REVISED THRESHOLDS TO REPORT:

1. Serious Threat
2. Allegiance to the U.S.
3. Espionage/Foreign Considerations
4. Personal Conduct
5. Behavioral Considerations
6. Criminal Conduct
7. Unauthorized Disclosure
8. Unexplained Personnel Disappearance
9. Handling Protected Information
10. Misuse of Information Technology
11. Terrorism
12. Criminal Affiliations
13. Adverse Clearance Actions


[ADD CLASSIFICATION RATING HERE]

[DOD Component] Insider Threat Datasheet v1.03

	Component Case # (Required) — This is the local component case identification number or text	Text	
	DITMAC Case # (Do Not Complete) — This is the local component case identification number or text	Text	
Primary Actor Information	**Primary Actor Person Information**		
	1 Gender (Required) — Reference to the Gender for the Person – e.g. Male, Female	List	
	2 Primary Citizenship — Reference to the country for the person's primary citizenship	List	
	3 Secondary Citizenship — Reference to the country for the person's secondary citizenship	List	
	Primary Actor Clearance Information		
	4 Eligibility — Eligibility	List	
	5 Access — Active clearance "in access" in JPAS	List	
	6 Issued Date — Date Clearance was originally issued	Date (MM/DD/YYYY)	
	7 Clearance Organization — Issuing organization	List	
	Primary Actor Organization Assignment		
			Primary
	8 Affiliations (Required) — The "Primary" Affiliation column describes the DoD Component entity that an individual belongs to (could be a Component analyst or an individual that is the subject of a Case. The other columns can be used to list any	List	
	9		
	10		
	11		
Case	Com		
	12		
	13		
	14		
	15		
	16 — Reference to the Case Status – e.g. New, In Progress, On Hold, Pending Approval, Pending Adjudication, Adjudicated, Closed	List	
	17 Case Close Date — Date case was finalized and closed out	Date (MM/DD/YYYY)	
Component Tasks	**Component Action Items**		
	18 Organization — The organization performing the action	List	
	19 Action Summary — The summary description of the action taken.	Text	

[ADD CLASSIFICATION RATING HERE]

HOW TO REPORT:

Submit PRI on SIPR to

dss.ncr.dss-ci.mbx.ditmac-ops@mail.smil.mil

Current Operations and Reporting

☑ DITMAC can receive Component InT reports today

- All Components were given datasheet (spreadsheet) for reporting
- Components can submit datasheet via SIPR email
- No PII/PHI can be sent to DITMAC until SORN is in place
- Reporting is based on 13 initial thresholds

☑ DITMAC is conducting basic analysis

- We are receiving PRI reports that meet threshold requirements
- We are identifying and sending media reports to Components

☑ DITMAC is providing basic metrics to DoD leadership

- Component reporting will build the DoD InT enterprise view

What DITMAC Will/Will Not Do

☒ **DITMAC will NOT:**

- Supersede or run the DoD Component InT programs
- Direct Components to take action on its people
- Take actions against any Component's people
- Allow analysis to be dominated by a single discipline
- Set Insider Threat policy

☑ **DITMAC will:**

- Support and enable Component InT Programs
- Identify InT challenges and develop solutions
- Promote best practices across Component programs
- Leverage a team of cross-functional subject matter experts (SMEs)
- Advocate for Components to OUSD(I) on policy ideas and initiatives

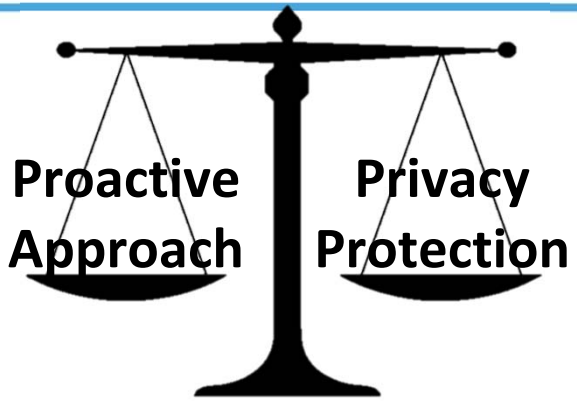
Protecting and Advancing our Values

"It's not enough to employ measures to protect classified information. It's not enough to prevent unauthorized disclosures. And it's not enough to position our programs to protect against employees who intend to do violence. We also have to protect the civil liberties and privacy of our employees. That's not a point I'm willing to compromise on."

-- Hon. James R. Clapper, Director of National Intelligence

Remarks at National Insider Threat Task Force Legal Forum, October 28, 2015

How DITMAC Advances DoD Missions



- **TRUST:** DoD missions depend upon safety and security
- **ENTERPRISE CAPABILITY**: DoD requires an enterprise InT capability to mitigate the risk of insidious insider threats
- **COORDINATION:** DITMAC is DoD's Hub to support and enable Component Hubs and senior DoD InT leaders
- **ANALYSIS:** DITMAC works with Hubs to identify and analyze behaviors indicative of a potential insider threat
- **MULTI-DISCIPLINARY:** DITMAC's diverse team of experts leverage advanced analytics and unique data sources

Conclusion

Q) How should we measure the effectiveness of our insider threat programs?

A) We must always ask ourselves, “Are we…”

☑**Protecting our people**

☑**Safeguarding their trust**

☑**Securing our resources**

DITMAC will enable DoD and its Components to meet this vital imperative, together with you.

Insider Threat Awareness Training Products

Related Training

- Establishing an Insider Threat Program
- Insider Threat Awareness

Job Aids

- Insider Threat Case Studies
- Insider Threat Toolkit

Past Webinars

- Insider Threat for DoD
- Cyber Insider Threat

http://www.cdse.edu/catalog/insider-threat.html

Question and Answer Session

DITMAC@dss.mil or (571) 357-6850

Counterintelligence Training POC:

Peter DeCesare and Rebecca Morgan

(410) 689-1136 (410) 689-1294

Email: counterintelligence.training@dss.mil