*Operating with Integrity*

**CULTURE OF EXCELLENCE**

# SECURITY UPDATES

**Chris Mick**
**Security Manager/FSO**
**Eagle Applied Sciences**
**Government Services Group**

*Operating with Integrity*

# CULTURE OF EXCELLENCE

-SECURITY CLEARANCES

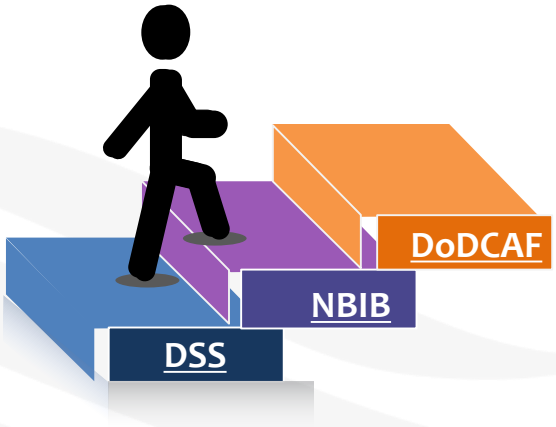
- FACILITY CLEARANCES

-INSIDER THREAT

# SECURITY CLEARANCES

*-Timelines*
*-JPAS Replacement*
*-E-Qip Changes*
*-Continuous Evaluation*

# INDUSTRY PERSONNEL CLEARANCE TIMELINESS

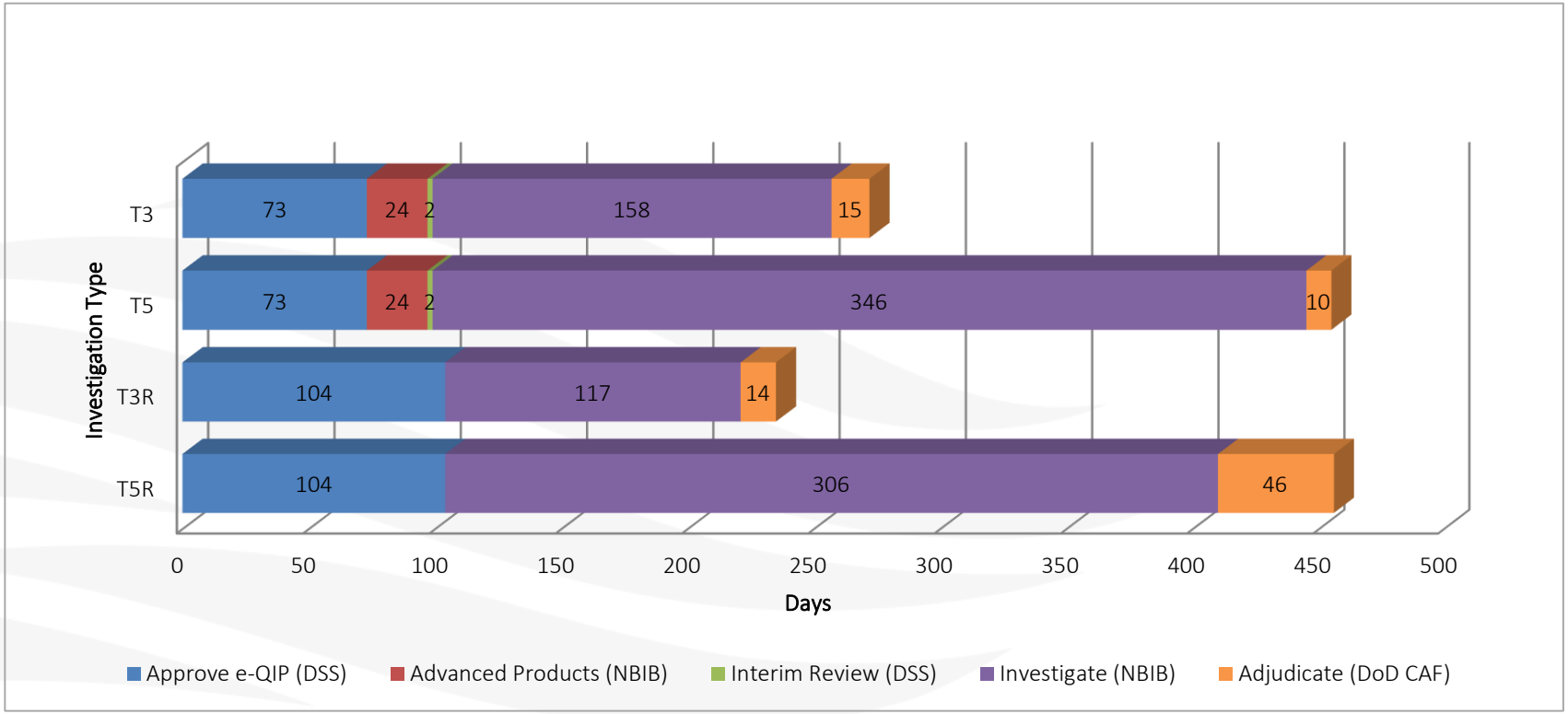



**DSS**
Review e-QIP and determine interim eligibility

**NBIB**
Schedules and completes investigation

**DoDCAF**
Reviews completed investigation against adjudicative guidelines

# INDUSTRY PERSONNEL CLEARANCE TIMELINESS



# JOINT PERSONNEL ADJUDUCATION SYSTEM (JPAS) REPLACEMENT

*Defense Information System for Security (DISS)*

The Defense Information System for Security (DISS), once fully deployed, will replace the Joint Personnel Adjudication System (JPAS), to serve as the system of record to perform comprehensive personnel security, suitability and credential eligibility management for all Military, civilian, and DOD contractor personnel. DISS provides secure communications between Adjudicators, Security Officers and Component Adjudicators in support of eligibility and access management. DISS will deploy in a phased approach, with Phase 1 (DISS 1.0) being rolled out to users incrementally, starting with WHS and ending with Industry

# E-QIP/SF-86 CHANGES (AUGUST 2017)

- **Section 12** - **Where You Went to School** - added link to assist determining school
- **Section 21** - **Psychological and Emotional Health** - includes vastly different questions than previous versions as a result of a comprehensive review to clarify mental health treatment and to encourage proactive management of mental health conditions to support wellness and recovery. It is important to note that mental health treatment and counseling, in and of itself, if not a reason to determine the suitability or fitness for federal or contract employment, or to determine the eligibility for access to classified information, for holding a sensitive position, or for physical or logical access to federally controlled facilities or information systems.
- **Section 23** - **Illegal Use of Drugs and Drug Activity** - includes a statement that "illegal use" is in accordance with Federal laws, even though permissible under state laws.
- **Section 26** - **Financial Record** - added Chapter 12 Bankruptcy.
- **Certification** - added words to affirm that classified information is not provided on the form

# CONTINUOUS EVALUATION PROGRAM

**Social networks** (examples include myspace, Facebook, and LinkedIn)

**Micro-blogging websites** (examples include twitter and StumbleUpon)

**Blogging and Forums websites** (examples include WordPress, tumblr, and LIVEJOURNAL)

**Pictures and Video-Sharing websites** (examples include YouTube, flickr, and Flikster)

**Music websites** (examples include Pandora, lost.fm, and iLike)

**Online Commerce websites** (examples include eBay, amazon.com, and Epinions)

**Dating Network websites** (examples include match.com, eHarmony, and chemistry.com)

**Geo Social Network websites** (examples include foursquare, urbanspoon, and tripadvisor)

**News and Media websites** (example include the LA Times, CNN, and New York Times)

# FACILITY CLEARANCES

National Industrial Security System (NISS)

# E-FCL AND ISFD REPLACEMENT

*National Industrial Security System*

It will replace ISFD and e-FCL, and be used for Facility Clearance Sponsorship Request submissions, Facility Clearance Verifications, Facility Clearance Package Submissions, Annual Self Inspection Certifications, reviewing information associated with your facility, and reporting of Change Conditions, Security Violations, and Suspicious Contact Reports.

# INSIDER THREAT

*2015 – 48 percent of Cyber Breaches*

*2016 – 60 Percent of Cyber Breaches*

# THE DANGER OF INSIDER THREATS

According to a 2017 Insider Threat Report, 53 percent of companies estimate remediation costs of $100,000 and more, with 12 percent estimating a cost of more than $1 million. The same report suggests that 74 percent of companies feel that they are vulnerable to insider threats, with seven percent reporting extreme vulnerability.

- **Insider threats can go undetected for years**
- **It is hard to distinguish harmful actions from regular work**
- **It is easy for employees to cover their actions**
- **It is hard to prove guilt**

# THE CAUSE OF INSIDER THREATS

While any employee can cause a data misuse or leak by mistake, the three groups that you should give the most attention to are:

- **Privileged users** – These are usually the most trusted users in a company but they also have the most opportunities to misuse your data, both intentionally and unintentionally.
- **Third parties** – Remote employees, subcontractors, third-party vendors and partners all usually have access to your system. Since you know nothing about the security of their systems and often even about the very people accessing your data, you should treat them as a security risk.
- **Terminated employees** – Employees can take data with them when terminated. Even more importantly, sometimes they can access your data even after termination, either via malware or backdoors or by retaining their access because nobody bothered to disable it.

# FIGHTING INSIDER THREATS

These are the steps every company should take in order to minimize insider threats:

- **Background checks**
- **Watch employee behavior**
- **Use the principle of least privilege**
- **Control user access**
- **Monitor user actions**
- **Educate employees**


# THANK YOU

*Operating with Integrity*

## CULTURE OF EXCELLENCE

**Chris Mick**

**Security Manager/FSO**

**(210) 581-9685**

**Chris.mick@eagle-app-sci.com**