Session #26

What Happens at the Department When There is a Cybersecurity Breach?

Robert Ader, Dan Commons, and Tom Harper
U.S. Department of Education

2019 FSA Training Conference *for Financial Aid Professionals*

December 2019

Panel Speakers:

Robert Ader – Department of Education, Cyber Operations Branch Chief

Tom Harper, Jr. – Office of Inspector General (ED OIG), Special Agent in Charge, Technology Crimes Division

Dan Commons – Federal Student Aid, Enterprise Director, Information Technology Risk Management / Chief Information Security Officer (CISO)

Dan Commons

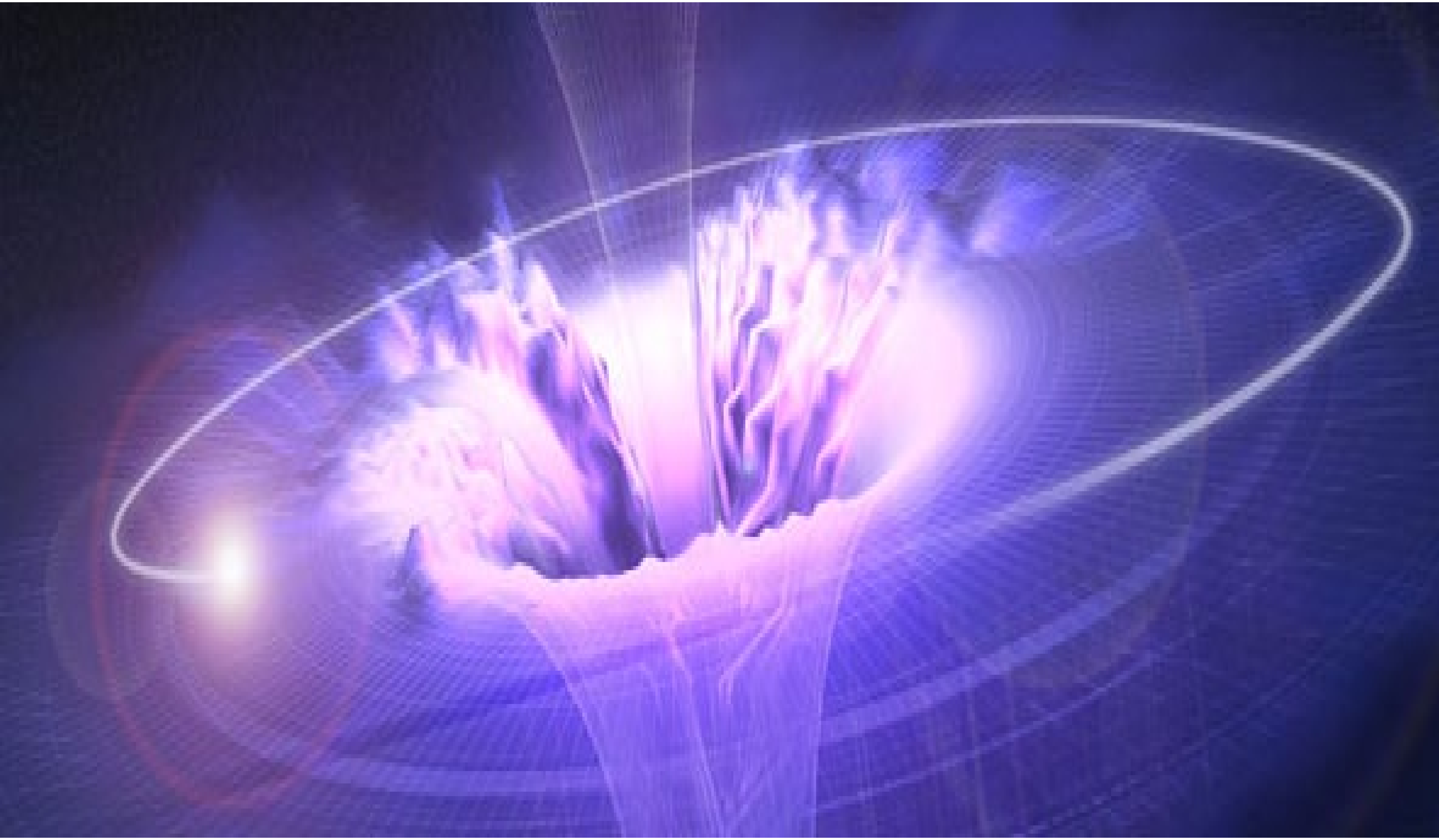
Federal Student Aid
An OFFICE of the U.S. DEPARTMENT of EDUCATION

PROUD SPONSOR of
the AMERICAN MIND®

Director of Information Technology Risk Management

Chief Information Security Officer (CISO)

The Black Hole



FSA AT A GLANCE

Investing in Cybersecurity and Privacy Protection

FSA holds personally identifiable information for **42M customers** and ensures the security of systems that manage **$1.5T in loans**

Working with Partners to Protect Data

- Responding to the 403% increase in school breach reporting since 2017
- Providing cybersecurity guidance for 6,000 schools and the student aid industry
- Assessing the security controls of 22 Guaranty Agencies every 2 years

Increasing Threat Intelligence Capabilities

- Expanding the PSI Security Operations
- Educating and Increasing the cybersecurity workforce

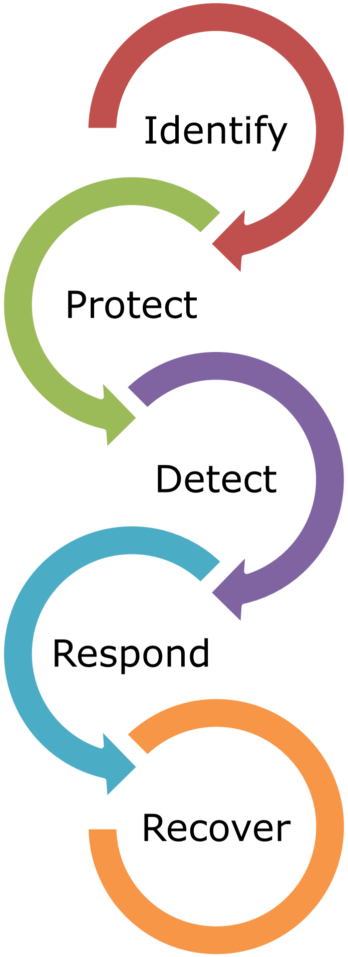
Expanding Risk-Based Security Practices

- Providing continuous assessment of the authority to operate for 69 systems
- Expanding the oversight and security reviews of 8 critical High Value Assets (HVAs)

Enhancing Security Governance

- Building cybersecurity best practices into NextGen FSA
- Responding to constantly evolving security requirements and guidance
- Implementing standardized security requirements for all IT acquisitions

Education’s Partnership with PSI’s



LEFT

Identify

Cybersecurity Guidance

Protect

Safeguard Guidance

BOOM

Detect

Incident Report, Intake, & Investigation

RIGHT

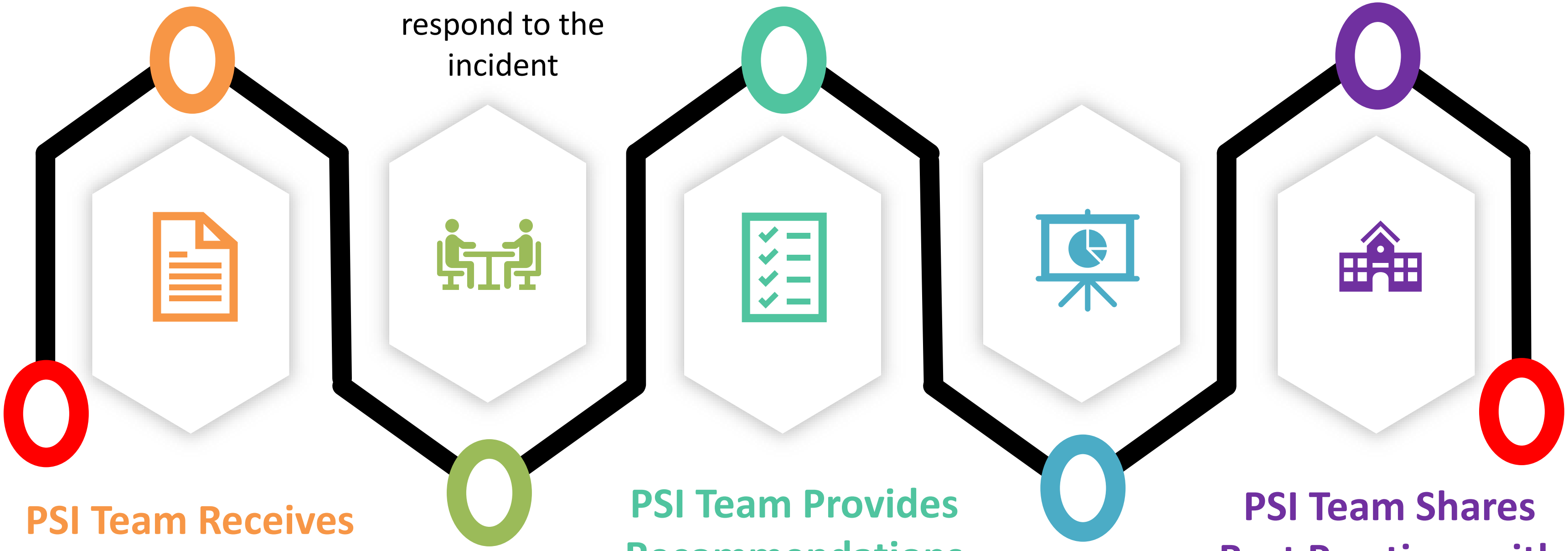
Respond

Containment Assistance, Root Cause Analysis, Site Visit, & Remediation

Recover

Fully system recovery and strengthening of security posture. Review of lessons learned and implementation of cyber practices.

FSA's PSI Breach Process



01

PSI Team Receives Incident Report

Incident is Analyzed & Classified

02

PSI Team Collaborates

Works with the school to triage and respond to the incident

03

PSI Team Provides Recommendations

Ensures Remediation is Complete

04

PSI Team Gathers Lessons Learned

Analyzes Trends

05

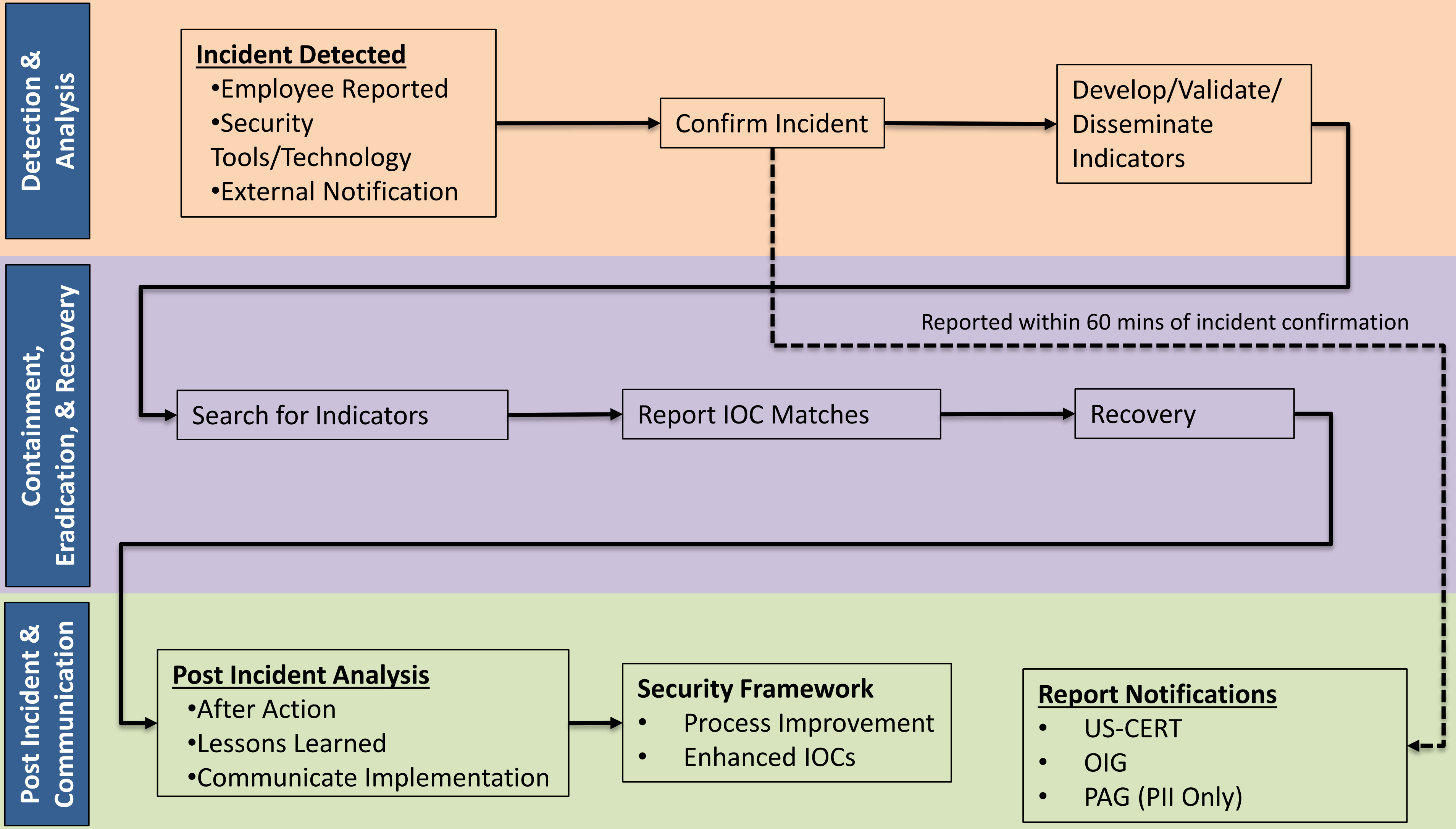
PSI Team Shares Best Practices with Schools

Incident Closed

Rob Ader

Department of Education, Cyber Operations Branch Chief

Incident Response Life-Cycle



Detection & Analysis

Incident Detected

- •Employee Reported
- •Security Tools/Technology
- •External Notification

Confirm Incident

Develop/Validate/ Disseminate Indicators

Reported within 60 mins of incident confirmation

Containment, Eradication, & Recovery

Search for Indicators

Report IOC Matches

Recovery

Post Incident & Communication

Post Incident Analysis

- •After Action
- •Lessons Learned
- •Communicate Implementation

Security Framework

- Process Improvement
- Enhanced IOCs

Report Notifications

- US-CERT
- OIG
- PAG (PII Only)

CISO Initiatives

Strengthening Through Collaboration

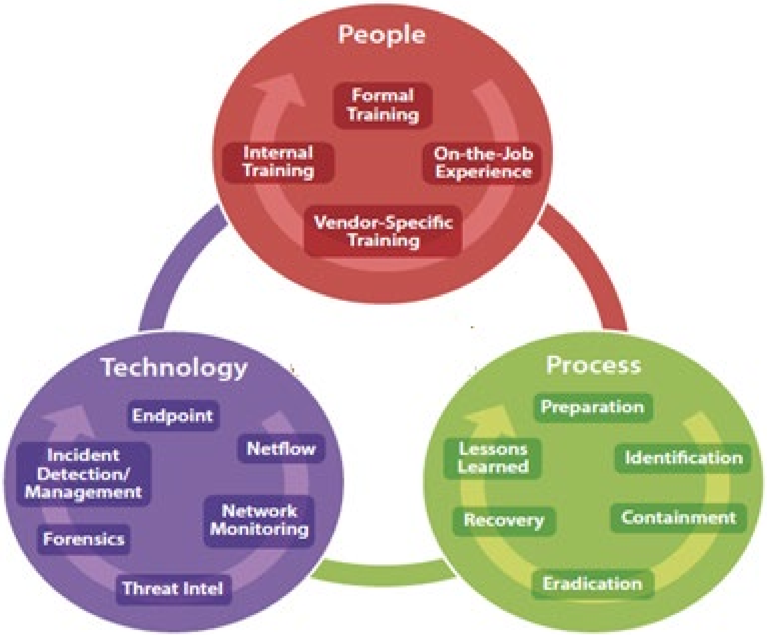
DoED CISO

Industry Partners

Federal Councils

FSA CISO

Enhancing Through Investments



People

- Formal Training
- On-the-Job Experience
- Vendor-Specific Training
- Internal Training

Process

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Technology

- Endpoint
- Netflow
- Network Monitoring
- Threat Intel
- Forensics
- Incident Detection/ Management

Tom Harper, Jr.

Office of Inspector General (ED OIG), Special Agent in Charge, Technology Crimes Division

What is an OIG?

- Independent component of Federal agencies
- Created by Congress
- Reports to Head of the Agency and Congress
- Inspector General appointed by the President and confirmed by the Senate
- An OIG's mission, generally: to audit and investigate agency programs and operations, promote economy, efficiency and effectiveness, and prevent and detect fraud and abuse

Technology Crimes Division

- Investigate crimes and criminal cyber threats against the Department's IT infrastructure, or
- Criminal activity in cyber space that threatens the Department's administration of Federal education assistance funds
  - Investigative jurisdiction encompasses any IT system used in the administration of Federal money originating from the Department of Education.

Case Examples

- Grade hacking
- Computer Intrusions
- Criminal Forums online selling malware
- ID/Credential theft to hijack Student Aid applications
- Business Email Compromise
- Misuse of Department systems to obtain personal information
- Falsifying student aid applications by U.S. government employees
- Child Exploitation material trafficking

Questions and Answers