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
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

Director of Information Technology Risk Management

Chief Information Security Officer (CISO)
The Black Hole
FSA AT A GLANCE

Investing in Cybersecurity and Privacy Protection

- 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

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

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

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

- 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

Identify
Cybersecurity Guidance

Protect
Safeguard Guidance

Detect
Incident Report, Intake, & Investigation

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 Collaborates
Works with the school to triage and respond to the incident

02 PSI Team Receives Incident Report
Incident is Analyzed & Classified

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
Department of Education, Cyber Operations Branch Chief
CISO Initiatives

Strengthening Through Collaboration

- DoED CISO
- FSA CISO
- Industry Partners
- Federal Councils

Enhancing Through Investments

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

- Technology
  - Endpoint
  - Netflow
  - Incidence Detection/Management
  - Forensics
  - Network Monitoring
  - Threat Intel

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