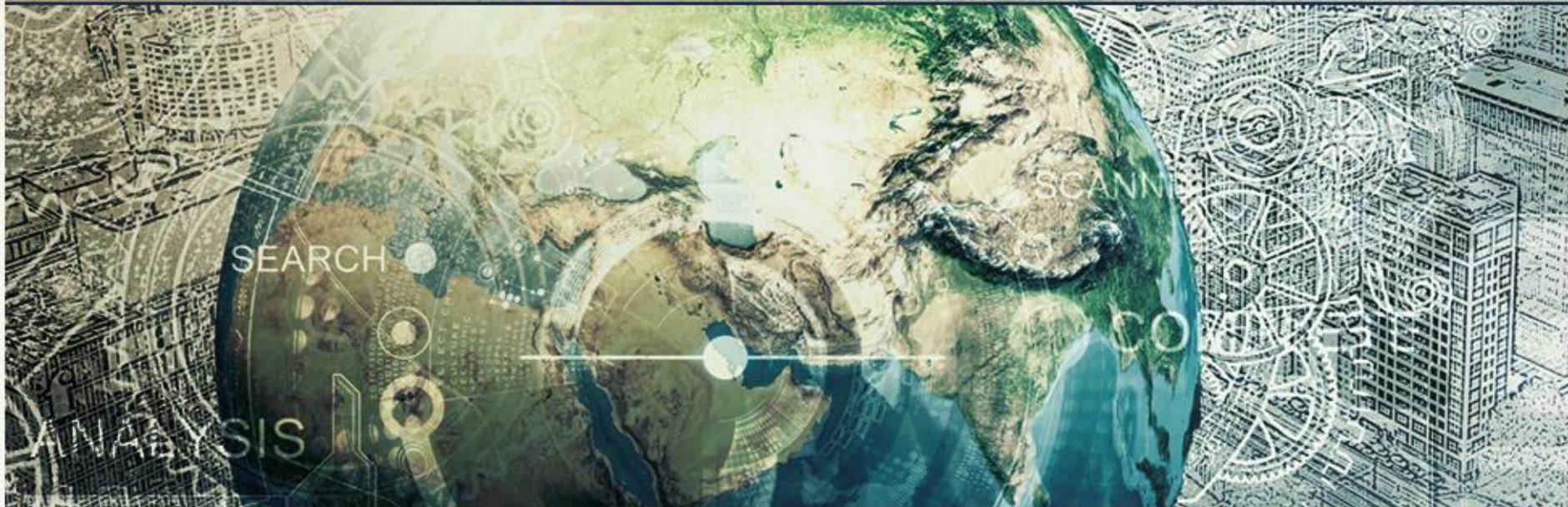


20th ANNUAL



Defense Security Service

FOCI CONFERENCE





Defense Security Service
FOCI CONFERENCE

DANIEL PAYNE

Director

Defense Security Service



THE NEW NORMAL

- **Overseas Headquarters**

- Multinational corporations
- **298** FOCI facilities; **\$18B** in 2015 sales
- * Risks: illicit influence, information leaks, supply chain infiltration



- **Investment Vehicles**

- Financial organizations or individuals
- **177** facilities; **\$4.1B** in 2015 sales
- * Risks: structured acquisitions, hidden influence



- **Foreign Governments**

- Companies and sovereign wealth funds
- **28** facilities; **\$2.6B** in revenue
- * Risks: foreign intelligence targeting





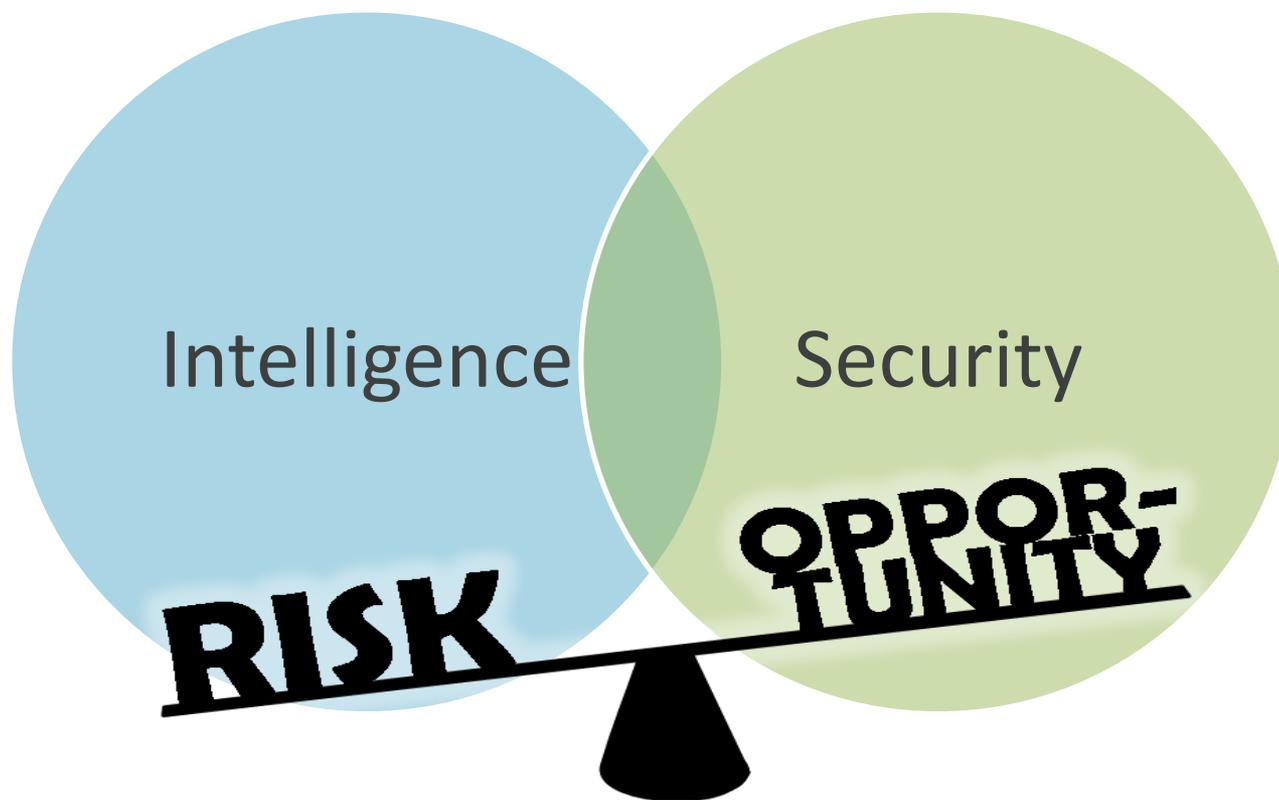
RISK BASED ANALYSIS AND MITIGATION



- 1 • Identify what we need to protect
- 2 • Determine plausible threat scenarios
• Rate impact of loss
• Use threat, impact of loss and vulnerability
- 3 • Determine if risk can be mitigated
• Re-evaluate impact of loss, and vulnerability
- 4 • Engage with stakeholders and partners to implement mitigation strategy
- 5 • Continuously evaluate results of risk mitigation

$$\text{Risk} = f\{\text{Threat, Vulnerability, Impact}\}$$

INTEGRATING INTELLIGENCE & SECURITY



CYBER THREAT



NBC NEWS HOME TOP VIDEOS DECISION 2016 ONGOING: EUROPE
U.S. WORLD LOCAL POLITICS HEALTH TECH SCIENCE POP CULTURE BUSINESS INVESTIGATION

TECH
APR 12 2016, 8:54 AM ET

Cyber Threats Are Getting Smarter: Report

by HERB WEISBAUM

Rafe Swan / Getty Images

SHARE

Share

Tweet

Share

Email

Print

Comment

The technology you use is being targeted, every hour of every day. These digital attacks are growing in number and sophistication, according to the Internet Security Threat Report released by the Cybersecurity and Infrastructure Security Agency on Tuesday. The data lost, the money spent, and the damage caused by cybercriminals is worse than ever.

"We see a higher level of professionalization in cyberattacks, not just nation states where you expect that sophisticated actors, but also cybercriminals," said Kevin Haley, director of the agency.

Cybercrime is now such a part of everyday life that the staggering numbers being reported are no longer surprising. More than 430 million new and unique pieces of malware were reported from the year before.

FOX NEWS Politics

Politics Home Elections 2016 Executive Senate House Defense Judiciary Fox News Poll

FBI warns of cyber threat to electric grid

By Bill Gertz · Published April 11, 2016 · Washington Free Beacon

Three months after a Department of Homeland Security intelligence report downplayed the threat of a cyber attack against the U.S. electrical grid, DHS and the FBI began a nationwide program warning of the dangers faced by U.S. utilities from damaging cyber attacks like the recent hacking against Ukraine's power grid.

The nationwide campaign by DHS and the FBI began March 31 and includes 12 briefings and online webinars for electrical power infrastructure companies and others involved in security, with sessions in eight U.S. cities over the next week in Washington.

Trending in Politics

1 Fresh document trove sheds light on Clinton-Trump ties

cy·ber·threat
/'sīber, THret/
noun
noun: cyber-threat

the possibility of a malicious attempt to damage or disrupt a computer network or system.
"the FBI has opened an investigation to address the potential cyberthreat"



INTEGRATING DOD AND THE INTEL COMMUNITY



Plus 31 executive branch agencies

A large, faint, grey world map is centered in the background of the slide. The text "QUESTIONS & COMMENTS" is overlaid on the map in a dark teal color.

QUESTIONS & COMMENTS



Defense Security Service
FOCI CONFERENCE



2016 FOCI CONFERENCE

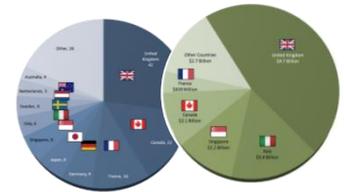
Fred Gortler
Industrial Security
Integration and
Application

UNPRECEDENTED INNOVATION AND RIGOR



- **DSS is modernizing its business analysis capabilities**

- Using financial models to understand FOCl
- Deploying new tools and methods



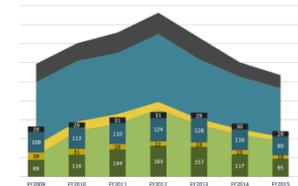
- **FOCl mitigation balances risk and opportunity**

- Risks of compromise or loss
- Opportunities for U.S. military advantage



- **In an era of consolidation, DSS must be agile**

- Not all FOCl is created equal
- Mitigation must match the risk





GLOBALIZATION IMPACT ON NISP IN 2016



QUICK FACTS:

- 31** Countries
 - 240** Agreements
 - 535** Facilities
 - \$25B** Revenues
- 95** Board Resolutions
 - 18** Security Control Agreements
 - 99** Special Security Agreements
 - 28** Proxy Agreements

AGENDA



0830 – 0900 Welcome

Daniel Payne, DSS Director

0900 – 0915 Conference Overview

Fred Gortler, Director, Industrial Security Integration and Application

0915 – 1015 Delivering Uncompromised

William Stephens, Director, Counterintelligence

Panel: Patrick Joyce
Harvey Rishikof
Carrie Wibben

1015 – 1030 Break

1030 – 1115 Risk & Competition in the
Global Marketplace

Nicoletta Giordani, Assistant Director, Industrial Security Integration and
Application, Business Analysis & Mitigation Strategy

Panel: David Carey
Barbara McNamara
Gen. Thomas Moorman, USAF (Ret.)
Hon. Dov Zakheim

1115 – 1215 Keynote Address

Maynard A. Holliday, Special Assistant
Office of the Under Secretary of Defense
for Acquisition, Technology and Logistics

1215 – 1315 Lunch

AGENDA



1315 – 1400	Risk Based Analysis & Mitigation	Fred Gortler Mike Halter, Deputy Director, Industrial Operations Kevin Jones, Director, CDSE William Stephens
1400 – 1415	Break	
1415 – 1445	Affiliated Operations Plan	Nicoletta Giordani
1445 – 1515	Behaviors in the Cyber Domain Impacting the NISP	Richard Naylor, Dep. Director, CI Cyber Operations
1515 – 1600	Operations Update	Keith Minard, Assistant Director NISP Administration and Policy Analysis Micah Komp, Quality Assurance Manager



FOR WANT OF A NAIL





QUESTIONS & COMMENTS



Defense Security Service
FOCI CONFERENCE

**DELIVERING ANALYSIS
UNCOMPROMISED**



DELIVERING UNCOMPROMISED

- Moderator
 - William Stephens
- Panel Members:
 - Patrick Joyce
 - Harvey Rishikof
 - Carrie Wibben

REASONABLE PREMISE



Fact: There are threats inside the wire of government and cleared industry

- American citizens expect defense and national security systems delivered intact and fully mission capable – Uncompromised
- Americans do not accept that technology is lost, stolen, sold or otherwise given away to our adversaries during the acquisition process

Fact: We ARE LOSING our vital technological advantage

- Industrial Security must not continue to be treated as a cost to be reduced, but rather as a National Security objective to be achieved as part of the acquisition
- Industrial Security Risk Management must be elevated to be on par with development and delivery program considerations to ensure technology is protected from compromise or loss during all phases of the acquisition life cycle

A NEW APPROACH: A SHARED RESPONSIBILITY



The government will...

- Require/pay for cleared industry security risk management program included in RFP process
- The USG will employ financial incentives/disincentives to stipulate uncompromised delivery

The prime contractor will...

- establish a risk management committee chaired by the CEO
- commit to maintaining an effective security risk management program across the life cycle
- field the ability to detect and promptly report all threats/vulnerabilities
- field the ability to develop and implement mitigations
- unilaterally refresh systems, processes and people to ensure state of the art risk management capability w/o being directed by the USG
- field the capability to internally red team processes, systems and people...and facilitate USG red teaming
- indemnify the USG if the prime/sub is found culpable for information / technology being lost, stolen, sold or otherwise given away



Defense Security Service
FOCI CONFERENCE



RISK & ANALYSIS
COMPETITION IN
THE GLOBAL
MARKETPLACE



RISK & COMPETITION IN THE GLOBAL MARKETPLACE

- Moderator:
 - Nicoletta Giordani
- Panel Members:
 - David Carey
 - Barbara McNamara
 - Gen. Thomas Moorman, USAF (Ret.)
 - Honorable Dov Zakheim

20th ANNUAL



Defense Security Service

FOCI CONFERENCE





Defense Security Service
FOCI CONFERENCE



RISK BASED ANALYSIS & MITIGATION

Fred Gortler
Michael Halter
Kevin Jones
William Stephens

RISK BASED ANALYSIS AND MITIGATION



$$\text{Risk} = f\{\text{Threat, Vulnerability, Impact}\}$$

(Terrorists, Criminals, Spies)

(People, Process, Systems)

(Lives, Dollars, Time)



Defense Security Service
FOCI CONFERENCE



**AFFILIATED ANALYSIS
OPERATIONS PLAN**

Nicoletta Giordani



AGENDA

1. AOP Guide for Industry
2. Identification of Affiliated Operations
3. AOP Submission and Acceptable/Unacceptable Examples
4. AOP Compliance and Best Practices
5. FOCI Training Update
6. Questions



AOP GUIDE FOR INDUSTRY

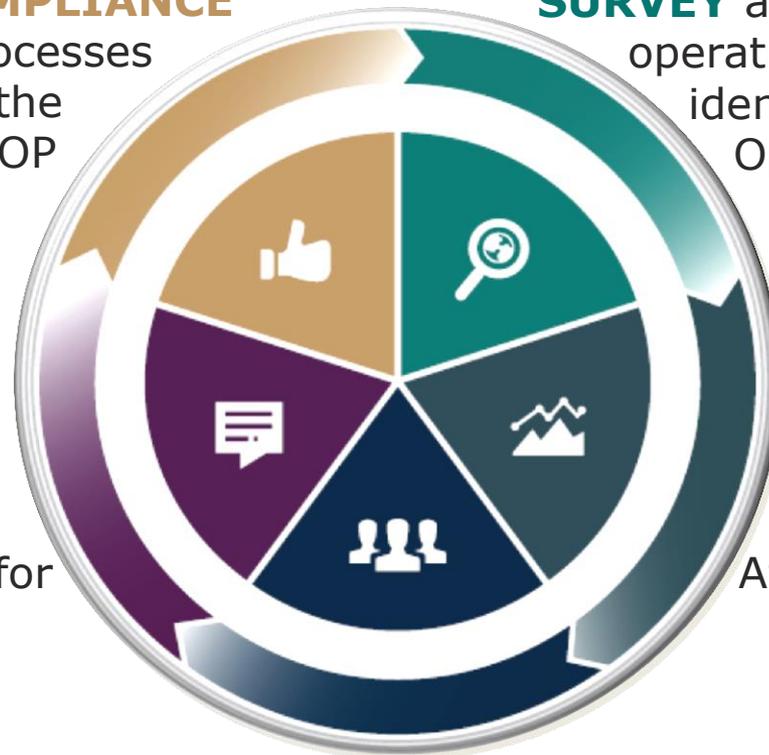
Ensure **COMPLIANCE** with the processes outlined in the approved AOP

SURVEY administrative and operational functions to identify Affiliated Operations

DESCRIBE Affiliated Operations, risks and mitigation in an AOP for DSS approval

Identify **RISKS** presented by each Affiliated Operation

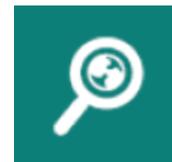
Work with relevant **EMPLOYEES** to develop risk mitigation measures



IDENTIFICATION OF AFFILIATED OPERATIONS



- The AOP provides transparency to DSS and the GSC about interactions and relationships between FOCI companies and their affiliates, to include:
 - Shared Services
 - Reversed Shared Services
 - Shared Employees
 - Shared Third-Party Services
 - Cooperative Commercial Arrangements
- From this potential risks can be identified:
 - Unauthorized access to classified or sensitive information.
 - Undue influence over the management and operations of mitigated companies.





AOP SUBMISSION

The guide describes how to develop the AOP, to include the following elements for each identified shared service:

1. Detailed description of the shared service.



2. Risks inherent in sharing the service.



3. Mitigation measures associated with shared service.



4. Review of the shared service, internally by the GSC, FSO, and TCO, and externally by DSS.



ACCEPTABLE AOP SUBMISSION: INTERNAL AUDIT



1. Service Description:



- The cleared company (Company) may work with the affiliate to scope the internal audit and receive guidance on the affiliate’s standard corporate practices.
- The focus of the audit will be financial reporting, operational performance, and compliance with pertinent laws and regulations.
- Internal audits are expected to take place annually.
- Company may submit the results of the audit to the affiliate for review.
- Company’s board will determine whether to accept or deny internal audit recommendations proposed by the affiliate.

ACCEPTABLE AOP SUBMISSION: INTERNAL AUDIT



2. Risks:



- Affiliate scoping, guidance, and review of audit report may result in:
 - Inadvertent disclosures of classified or other sensitive information.
 - Identification of cleared personnel and classified programs.
 - Compromise of company managerial independence.
 - Undue influence on process improvement recommendations impacting the performance of classified contracts.

ACCEPTABLE AOP SUBMISSION: INTERNAL AUDIT



3. Mitigation Measures:



- The company maintains an internal audit capability or may use a third-party internal audit provider. The affiliate will not directly participate in the company's internal audit.
- The cleared company's board will work with the affiliate to scope the internal audit and determine how to use the subject matter expertise.
- FSO/TCO will review the audit report and GSC will approve dissemination of final version to the affiliate.
- The cleared company's board will make the final decision on implementation of recommendations.

ACCEPTABLE AOP SUBMISSION: INTERNAL AUDITS



4. Review of Service:



- Documentation pertaining to the scope and standard corporate practices used for the internal audit.
- Board meeting minutes pertaining to internal audit (e.g. approval of scope, review of audit results, deliberation on improvement recommendations).
- Records pertaining to interactions related to the service (e.g. visitor requests, electronic communications)
- Copy of audit results submitted to the affiliates and records of FSO, TCO, and GSC approvals.

UNACCEPTABLE AOP SUBMISSION



1. Service Description:

- Affiliate will participate in the cleared company's internal audit.



2. Risk:

- There is no risk because classified information is not involved.
- This service presents no FOCI risks.

3. Mitigation Measures:

- The risk is mitigated by the FOCI mitigation agreement.
- The audit will be conducted by U.S. affiliate personnel

4. Review of Service:

- DSS may review any documents at any time.

AOP COMPLIANCE & BEST PRACTICES



- An AOP is a living document that requires continuous monitoring of new and existing shared services.
- When planning to integrate business functions and processes, resulting affiliated operations should be addressed before decisions are made.
- GSC should be involved in the development and maintenance of the AOP.
- Senior management should involve FSO for awareness of possible affiliated operations.
- Affiliated operations can be identified while reviewing electronic communications and visit requests.



FOCI TRAINING UPDATE

- DSS is developing three new training modules (4, 5, & 6) for Outside Directors and Proxy Holders





FOCI - Outside Directors, Proxy Holders, and Voting Trustees Training – Module 1

Module 1 Introduction to DSS and Foreign Ownership, Control, or Influence (FOCI)

Menu Transcript

▼ Module1

Module 1: Introduction

Module 1: Objectives

DSS Overview

Define FOCI

FOCI Factors

▼ FOCI Lifecycle

Mitigation Negotiation

▼ Mitigation Implementation

ECP Definition

TCP Definition

AOP Definition

FLP Definition

Visitation Plan Definition

Mitigation Oversight

Change Condition

Identification & Assessment

▼ Mitigation Instruments

Minority Ownership

Majority Ownership

Module 1: Conclusion



< PREV

NEXT >



QUESTIONS & COMMENTS



Defense Security Service
FOCI CONFERENCE



OPERATIONS UPDATE

Keith Minard
Micah Komp

OPERATIONS UPDATE



- NISPOM Change 2 (General Overview)
- Risk Management Framework (System Accreditation)
- Insider Threat Program Implementation and Management

NISPOM CHANGE 2, INSIDER THREAT



- What will be required?
- How do I implement my program?
- Company vs. Corporate Program
- DSS Resources and Tools
- The oversight question?



QUESTIONS & COMMENTS