



---

# **Justin Walsh**

## **FOCI Program Manager**

### **Industrial Security Field Operations**





# Briefing Objectives

---

- **FOCI Oversight Metrics**
- **Reasons for poor security ratings at FOCI Facilities**
- **FOCI Best Practices**
- **ECP**



# FOCI Oversight Data

---

- FY 2011, DSS has conducted 9,758 security reviews
- 303 of which were FOCI signatories
- Non-FOCI signatories Compliance Breakdown:
  - 77.4% rated Satisfactory
  - 17.5% rated Commendable
  - 4.6% rated Superior
  - 0.5% rated Marginal or Unsatisfactory
- FOCI Signatory Compliance Breakdown:
  - 68.3% rated Satisfactory
  - 23.4% rated Commendable
  - 7% rated Superior
  - 1.3% rated Marginal or Unsatisfactory



# Reasons for Poor Security Ratings

---

- Lack of management support for implementing the agreement
- Unauthorized Co-location
- Shared services occurring without approval
- Company not abiding by the visitation requirements of the agreement
- Inadequate monitoring of electronic communications
- Contact Reports not being logged or tracked
- Failure to report FOCI Changed Conditions



# Reasons for Poor Security Ratings

---

- Failure to submit an Annual Compliance Report
- Lack of security education training on the agreement
- GSC not implementing the provisions of the agreement
- Failure to implement a TCP or appoint a TCO
- Sending an export controlled document to an affiliate without proper export authority.



# FOCI Best Practices

---

- Strong GSC and Management support that are fully engaged on the requirements of the FOCI agreement and supportive of the security staff.
- Automated approach to auditing FOCI requirements
- Conducting FOCI Compliance trend analysis and tailoring compliance policies and education to the recent trends
- Review of 100% of electronic communications. Include a robust standard content review for electronic communications



# FOCI Best Practices

---

- **Outstanding security education programs which foster a culture of understanding and compliance with the agreement**
- **Conduct frequent self inspections across the company to ensure compliance with the FOCI agreement as well as NISP requirements.**
- **Security staff involved in Industry Groups focused on compliance with FOCI and other NISP requirements.**
- **Continuous communication with DSS to ensure transparency on matters pertaining to FOCI**



## ECP Template Summary of Changes

---

- Revised template released October 2011
  - [http://www.dss.mil/isp/foci/foci\\_info.html](http://www.dss.mil/isp/foci/foci_info.html)
- Clarification on Teleconference and Video Teleconference requirements (See sections 1, 17.1, and 17.3 of the ECP Template).
  - Teleconferences no longer treated as visits
- Monitoring configuration changes and defining which ECP changes require prior approval by DSS (See section 8.1 and the addition of attachment 4 "ECP Revision Log").





## ECP Template Summary of Changes

---

- Export Control Procedures (Section 16). The addition of the sentence: "If a third party provider is administering the Company's network, please describe the Company's procedures in place to ensure that export control violations do not occur with respect to the third party provider's administration of the Company's network."
- Attachment 3 - The User Acknowledgement language has been revised to reflect that employees must be briefed on the purpose of the ECP and their responsibilities under the plan.



## Common Reasons for ECP Rejections

---

- ECP missing required attachments such as network configuration diagrams and company policies and procedures referenced in the ECP.
- Section 17 Additional FOCl Procedures are either not filled out completely with adequate detail or their current procedures are not adequate.
- Inadequate Description of Technical Baselines.