International Space Agency CIO Forum
Industrial Control Systems (ICS) and Cyber

Robert Powell,
CISSP / CISM
Senior Advisor, Cybersecurity
May, 2017

www.nasa.gov
Discussion Areas

• Definition of OT
• NASA OIG Findings
• OCIO Focus
• Integrated Approach
• Top Weaknesses (ICS-CERT)
• Defense-in-Depth (Best Practices)
• NIST References
• ICS-CERT References
Operational Technology (OT) is hardware and software that detects or causes a change through the direct monitoring and / or control of physical devices and processes.

- Based on NIST & Gartner OT Definitions

OT Systems Include*:
- ICS (Industrial Control System)
- SCADA (Supervisory Control and Data Acquisition) System
- Distributed Control System
- Process Control System
- Building Automation/Control System
- Safety Instrumented System
- Logic Controllers

* Systems that do not qualify as OT include: Email systems, HR systems, SAP, etc.
Six Focus Areas:

1. Develop a framework to coordinate security efforts
2. Develop a standardized process to assess Agency cyber and physical assets for NASA critical infrastructure
3. OPS will include OCIO and OSI in assessments of critical infrastructure and facility security to appropriately address interdependencies
4. Coordinate development of a methodology for identification and protection of interdependencies
5. Develop security policy based on NIST guidance (800-53 and 800-82) for managing the protection of OT. At a minimum, this should include (subset listed below):
   a. Definition for ICS
   b. Strategy for segmenting OT from IT
   c. Develop system security plans and assessment methodologies
   d. Develop training for responsible security personnel
6. Establish an integrated cyber and physical risk management committee composed of subject matter experts from NASA Mission Directorates and Mission Support Offices (OCIO – Office of the Chief Information Officer, OPS – Office of Protective Services, OSI – Office of Strategic Infrastructure, OCE – Office of Chief Engineer)
OCIO Focus Areas

1. Develop a framework to coordinate security efforts across the Agency

2. Develop a standardized process to assess Agency cyber and physical assets for NASA critical infrastructure

3. Ensure appropriate Agency personnel are included in functional reviews of NASA’s critical infrastructure assets and facility security assessments

4. Coordinate the development of a methodology for the identification and protection of interdependencies

5. Develop security policy and procedures for managing the protection of OT that addresses key areas identified during this review

6. Establish an integrated cyber and physical risk management committee composed of SMEs from NASA Mission Directorates, OCIO, OPS, and OSI
Integrated Approach

OPS
Office of Protective Services
- Emergency Management
- Personnel Safety and Security
- Physical Security (inc. Counterterrorism)

OCIO
Office of CIO
- Compliance assessments
- Information Security
- IT Architecture/Engineering
- Policy instruments
- Technical Testing

ICSWG

OCE
Office of Chief Engineer
- Systems Engineering

OSI
Office of Strategic Infrastructure
- Capital Planning
- Energy Management
- Environmental Management
- Facilities Engineering

Missions
- Mission Success
- Requirements Management
- Risk Management

Procurement
- Contract management
- Policy framework
OCIO:
- Data Center Management Systems
- Land Mobile Radio
- Internet of Things
- Telephone systems

OSI:
- Building Automation / Management Systems
- Elevator Control Systems
- Energy Management Systems
- Fire Alarm / Sprinkler Systems
- Renewable Energy Control Systems

OPS:
- Intrusion Detection Systems
- Physical Access Control Systems
- Personnel Safety Support Systems
  - Emergency Alert Systems
  - Surveillance Systems (e.g., CCTV)

Mission:
- Antenna Control Systems
- Integration and Test Systems
- Laboratory and Research Chambers
- Range Safety and Launch Support
- Sensor networks
#1 Recommendation – Boundary Protection

- **Monitor and control** of ICS communications at external and key internal boundaries
- Implement **subnetworks** to separate critical systems
- Implement **managed protective interfaces** for external connectivity to critical systems
Layers of protection makes it difficult for an adversary to penetrate into critical assets.

Network segmentation avoids one big flat network.
NIST References


- NIST SP **800-53rev4**: Security and Privacy Controls for Federal Information Systems and Organizations (December 2014)

- NIST Information Technology Bulletin (ITL) for November 2015: Tailoring Security Controls for Industrial Control Systems
ICS-CERT References

- DHS Recommended Practice: *Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies* (September 2016)

  - [https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/MitigationsForVulnerabilitiesCSNetsISA_S508C.pdf](https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/MitigationsForVulnerabilitiesCSNetsISA_S508C.pdf)

- DHS Presentation: *Common Cybersecurity Vulnerabilities in Industrial Control Systems* (May 2011)
Questions?