TRUSTED CI

THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

trustedci.org

Standard Operating Procedures (SOPs) for IT/OT and Science

Trusted CI & OSU

Speaker: Chris Romsos, John Zage

Nov 3, 2025, RVTEC

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Trusted CI: The NSF Cybersecurity Center of Excellence

https://trustedci.org/

Our mission: The mission of Trusted CI is to enable trustworthy NSF science by partnering with cyberinfrastructure (CI) operators to build and maintain effective cybersecurity programs, publishing resources that are valuable to the broader NSF community, and supporting the processes, tools, and knowledge to secure NSF research progress.

CENTER FOR APPLIED CYBERSECURITY RESEARCH

BERKELEY LAB

PSC

ILLINOIS NCSA | National Center for Supercomputing Applications

WISCONSIN UNIVERSITY OF WISCONSIN–MADISON

Arizona State University

SUSTAINABLE HORIZONS INSTITUTE

TRUSTED CI THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Motivations

- RCRV:
  - will operate three new vessels in transition to operations
  - seeks to reduce cyber risk and duplicative work
  - strives for repeatable & predictable outcomes (get it right)
  - wants to contribute to securing our fleet

- TrustedCI:
  - Secure by Design mission- built into the design, continues through the use of SOP

Current State of SOPs in the ARF

- ISM Code (incorporated under SOLAS) Chapter IX
  - Safety Management System (U.S. regulation 33 CFR Part 96)
    - Must include procedures for safe operation
      - In effect SOPs for the relevant operations and emergencies,
      - Not for every task though

- UNOLS Research Vessel Safety Standards
  - Appendix B

- No universally adopted security SOPs in ARF

SOP Development Steps

1. Decide what systems need an SOP

1. Define your SOP Scope

1. Draft & Refine

1. Implement & Train

Step 1: Decide what systems need an SOP

- What operations could benefit from standardization of operation?
- Which regulatory requirements or policies call for an SOP?

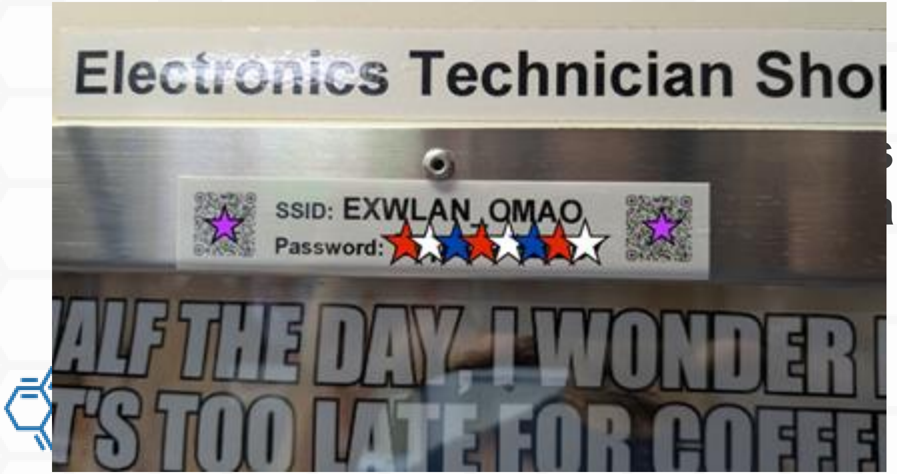
1. Secure Ship Wide Network Operation
    - 1.1. WAN
    - 1.2. Firewall
    - 1.3. Core
    - 1.4. Edge
    - 1.5. DNS
    - 1.6. DHCP
    - 1.7. Domain Controllers
    - 1.8. Wireless
2. Secure Computing Operation
    - 2.1. Virtualization Servers
    - 2.2. Application Servers & Workstations
    - 2.3. Digital Storage
3. Secure Scientific Data Systems
    - 3.1. Atmospheric
    - 3.2. Flowthrough
    - 3.3. Profiling
    - 3.4. Acoustic
    - 3.5. Navigation
    - 3.6. Data Acquisition
4. Secure OT Systems
    - 4.1. Integrated Bridge
    - 4.2. Overboard Handling

Decide what systems need an SOP

Example- 1: RCRV Secure Use of WiFi

How did we select where to start?

Started with something that was:



sky

ry

1. Secure Ship Wide Network Operation
   - 1.1. WAN
   - 1.2. Firewall
   - 1.3. Core
   - 1.4. Edge
   - 1.5. DNS
   - 1.6. DHCP
   - 1.7. Domain Controllers
   - 1.8. Wireless
2. Secure Computing Operation
   - 2.1. Virtualization Servers
   - 2.2. Application Servers & Workstations
   - 2.3. Digital Storage
3. Secure Scientific Data Systems
   - 3.1. Atmospheric
   - 3.2. Flowthrough
   - 3.3. Profiling
   - 3.4. Acoustic
   - 3.5. Navigation
   - 3.6. Data Acquisition
4. Secure OT Systems
   - 4.1. Integrated Bridge
   - 4.2. Overboard Handling

Step 2: Define Scope of a SOP

- Decide what subject matters are needed
- Decide who SOP applies to
- Decide what the Roles and Responsibilities are
- Which IMO/UNOLS requirements affect SOP

Define Scope of a SOP
Example- 2.1: RCRV Secure Use of WiFi

What areas of expertise are involved in developing a WiFi SOP?

Technical Experts	Network Architect, Network/System Administrator, Marine Techs
Security Experts	Cybersecurity specialist
Operational Experts	Captain/PortCaptain, IT Manager
End User Representative	Scientists, Crew
Risk Owners	CISO/CEO/CFO/Project Owner

Deciding Scope of a SOP
Example- 2.2-2.3: RCRV Secure Use of WiFi

To whom does this SOP apply?

This SOP applies to all personnel who use, manage, or maintain the 802.11 wireless network within the organization.

What are the roles and responsibilities for these personnel?

- ***Network Users*** - Adhere to acceptable use policy and report any suspicious activity.
- ***Network Admins*** - Configure/maintain the wireless network, enforce security policy, incident response
- **IT Security Team** - Monitor network security, perform audits, and ensure policy compliance.

Deciding Scope of a SOP
Example- 2.4: RCRV Secure Use of WiFi

Regulatory Requirements:

IMO MSC.428(98) 2017

Conduct CRMP & address cyber risks in your SMS

USCG Cybersecurity in the Marine Transportation System (2025)

Inspected vessels develop and maintain a cyber security plan

Step 3: Draft & Refine the SOP

- **Assemble your SMEs**
  - Pull in outside expertise if you have gaps!
- **Collect reference materials**
  - Technical & regulatory
- **Draft Procedures**
  - For your controls
- **Review/Revise**
  - Internal review (OSU)
  - External review (CIWG?)
- **Publish**
  - Internally
  - Externally

Draft & Refine SOPs
Example- 3.1: Choosing SMEs

What SMEs are needed to develop a WiFi SOP?

Technical Experts: Chris Romsos

Security Experts: Mikeal Jones, Drew Paine

Operational Experts: Don Hilliard (Port Engineer)

End User Representative: Joseph Soltis (OSU MarTech)

Risk Owners: Demian Bailey (Project manager)

David McMorries (OSU CISO)

Draft & Refine SOPs

Example- 3.2: Reference Materials

What SOPs for this already exist in the community or industry?

- No standard for WiFi SOPs, but guidance does exist

What guidance documents are available from commercial/govt sources?

- GCOS,
- Center for Internet Security Guide to Securing Networks for Wi-Fi (2017)
- NIST 800-153 (2012)
- Fortigate STIG

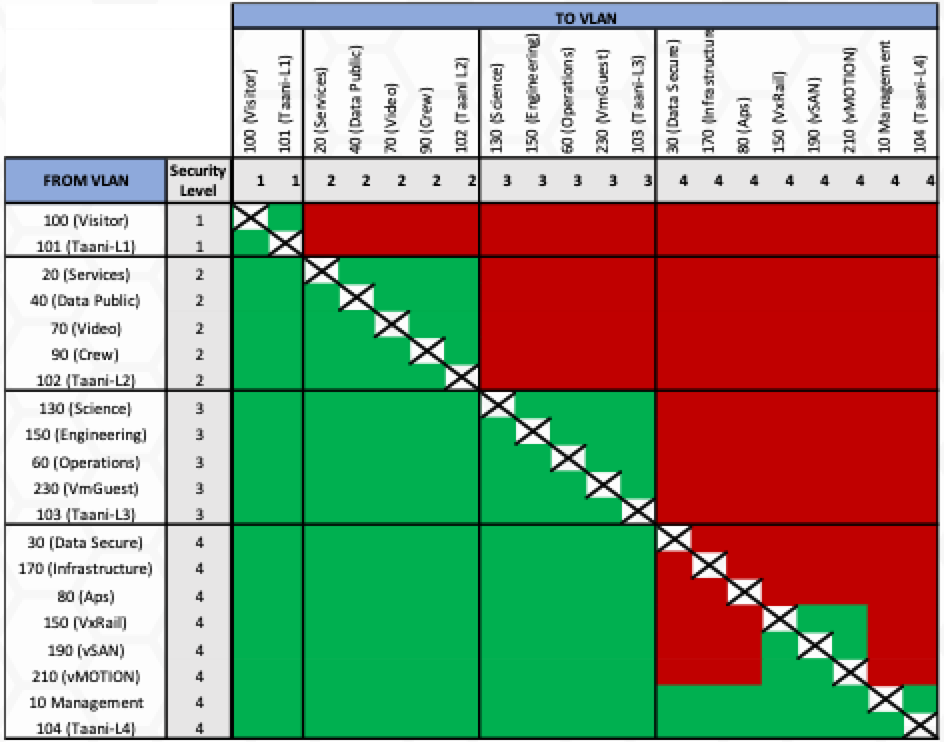
Draft & Refine SOPs
Example- 3.3: Drafting Procedures

What are the characteristics of a secure WiFi?

- Device configurations secured. (Fortigate Secure Technical Implementation Guide)
  - Controller Config
  - Access Point Config
- Devices are maintained
  - Patches applied regularly
- **Access controls are in place.**
  - **WPA3 Enterprise for secure network access**
  - **WPA3 SAE for public network access**
- **User Authentication**
  - **Password Policies in place**
- Network is Monitored for unauthorized access
- Infrastructure Data Protection - encryption between controller<->AP, WPA handles AP<->Device.

Draft & Refine SOPs
Example- 3.3: Drafting Access Controls

- Taani-L1 (VLAN 101)
  - Public access with a revocable credential
- Tanni-L2 (VLAN 102)
  - Authenticated L2 or higher users
- Taani-L3 (VLAN 103)
  - Authenticated L3 or higher users
- Taani-L4 (VLAN 104)
  - Authenticated L4 or higher users
- Taani-Video (VLAN 70)
  - Access restricted to AV devices fit for purpose, equivalent to L3.
  - SSID hidden



		TO VLAN																			
		100 (Visitor)	101 (Taani-L1)	20 (Services)	40 (Data Public)	70 (Video)	90 (Crew)	102 (Taani L2)	130 (Science)	150 (Engineering)	60 (Operations)	230 (VmGuest)	103 (Taani-L3)	30 (Data Secure)	170 (Infrastructure	80 (Aps)	150 (VxRail)	190 (vSAN)	210 (vMOTION)	10 Management	104 (Taani-L4)
FROM VLAN	Security Level	1	1	2	2	2	2	2	3	3	3	3	3	4	4	4	4	4	4	4	4
100 (Visitor)	1	☒	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
101 (Taani-L1)	1	🟩	☒	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
20 (Services)	2	🟩	🟩	☒	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
40 (Data Public)	2	🟩	🟩	🟩	☒	🟩	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
70 (Video)	2	🟩	🟩	🟩	🟩	☒	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
90 (Crew)	2	🟩	🟩	🟩	🟩	🟩	☒	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
102 (Taani-L2)	2	🟩	🟩	🟩	🟩	🟩	🟩	☒	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
130 (Science)	3	🟩	🟩	🟩	🟩	🟩	🟩	🟩	☒	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
150 (Engineering)	3	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	☒	🟩	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
60 (Operations)	3	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	☒	🟩	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
230 (VmGuest)	3	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	☒	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
103 (Taani-L3)	3	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	☒	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
30 (Data Secure)	4	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	☒	🟥	🟥	🟥	🟥	🟥	🟥	🟥
170 (Infrastructure)	4	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	☒	🟥	🟥	🟥	🟥	🟥	🟥
80 (Aps)	4	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	☒	🟥	🟥	🟥	🟥	🟥
150 (VxRail)	4	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	☒	🟩	🟩	🟥	🟥
190 (vSAN)	4	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟩	☒	🟩	🟥	🟥
210 (vMOTION)	4	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟩	🟩	☒	🟥	🟥
10 Management	4	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	☒	🟩
104 (Taani-L4)	4	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	☒

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Draft & Refine SOPs
Example- 3.3: Drafting Procedures

5.1. User Authentication:

- Ensure that there are 4 baseline password policies on the Fortigate, one for each security level.

- Open the Fortigate CLI and use the following code snippet to enable user password-policy “1” on the fortigate HA cluster.

```
config user password-policy
                edit "1"
                    set expire-days 90
                    set warn-days 7
                    set expired-password-renewal enable
                    set minimum-length = 8
                    set min-lower-case-letter 1
                    set min-upper-case-letter 1
                    set min-non-alphanumeric 1
                    set min-number 1
                    set min-change-characters 2
                    set expire-status enable
                    set reuse-password disable
                next
            end
```

Draft & Refine SOPs

Example- 3.3: Drafting Procedures

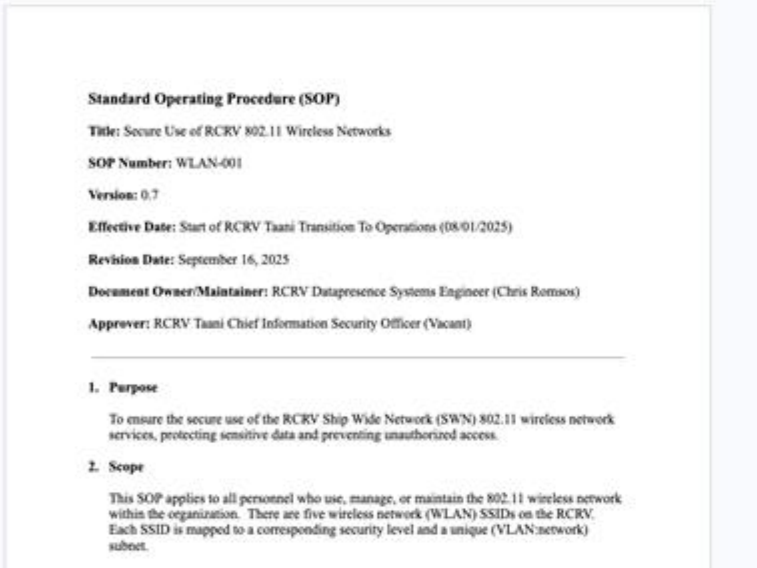
5.1. User Authentication (cont):

- Open the Fortigate CLI and use the following code snippet to enable user password-policy “2” on the fortigate HA cluster.

```
config user password-policy
                edit "2"
                    set minimum-length = 15
                    set min-lower-case-letter 1
                    set min-upper-case-letter 1
                    set min-non-alphanumeric 3
                    set min-number 3
                    set min-change-characters 2
                next
            end
```

Draft & Refine SOPs
Example- 3.4: Review/Revise

- Trusted CI Feedback from Secure by Design Team
  - Ensuring SOP matches best practices from Center for Internet Security (backup is NIST SP 800-153)



Standard Operating Procedure (SOP)

Title: Secure Use of RCRV 802.11 Wireless Networks

SOP Number: WLAN-001

Version: 0.7

Effective Date: Start of RCRV Taani Transition To Operations (08/01/2025)

Revision Date: September 16, 2025

Document Owner/Maintainer: RCRV Datapresence Systems Engineer (Chris Romsos)

Approver: RCRV Taani Chief Information Security Officer (Vacant)

1. **Purpose**

   To ensure the secure use of the RCRV Ship Wide Network (SWN) 802.11 wireless network services, protecting sensitive data and preventing unauthorized access.

2. **Scope**

   This SOP applies to all personnel who use, manage, or maintain the 802.11 wireless network within the organization. There are five wireless network (WLAN) SSIDs on the RCRV. Each SSID is mapped to a corresponding security level and a unique (VLAN:network) subnet.

Step 4: Implementation of a SOP

- SOPs are implemented through

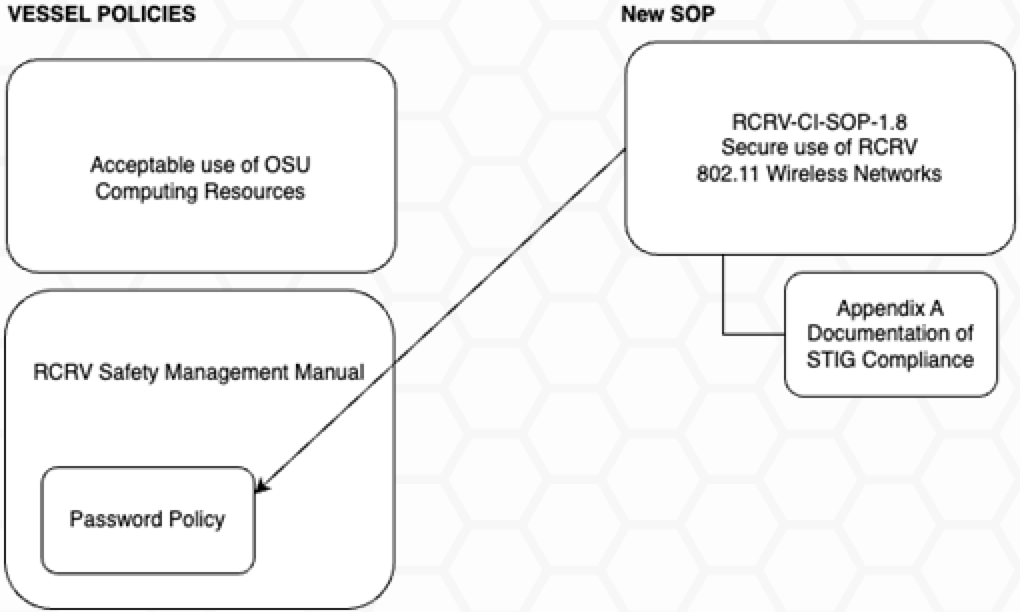
  - Formal ‘release’
    - may require sign-off, by whom & what level?
  - Policy adoption
    - may require connecting SOP to relevant Policies
  - Training of staff

SOP Implementation
Example- 4.1: Sign-off

- ‘Leadership’ accepts risks related to use of SOP
  - Sign-off from:
    - OSU’s Office of Information Security
    - OSU Ship Operations
    - Vessel Captain/Master

SOP Implementation
Example- 4.2: Policy Adoption

- Need to update any policies or procedures to reflect the existence of the new Secure use of WIFI SOP



VESSEL POLICIES

Acceptable use of OSU Computing Resources

RCRV Safety Management Manual

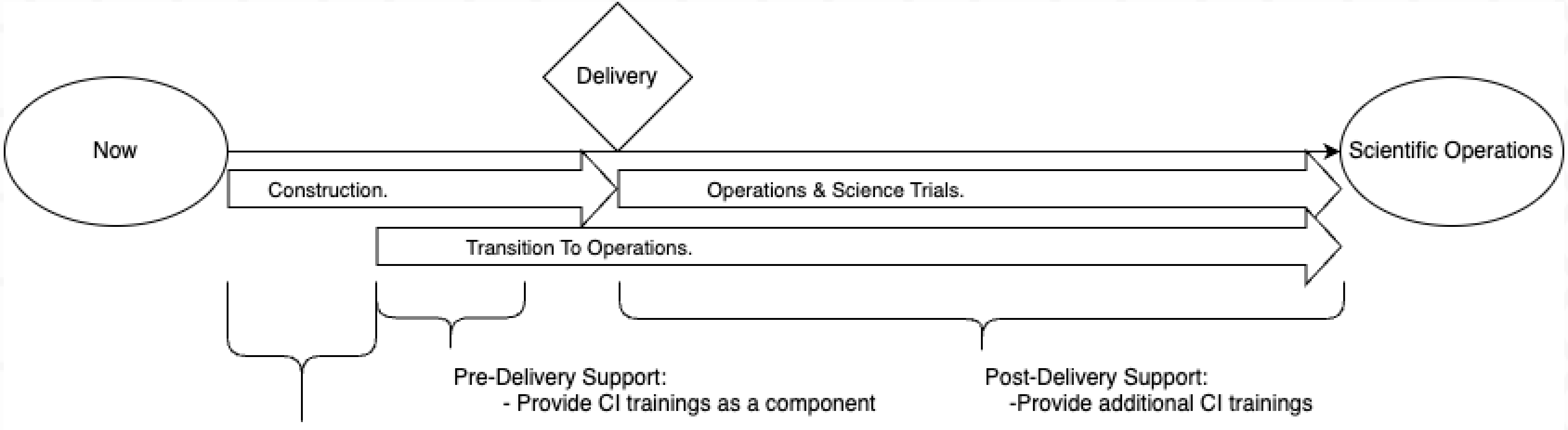
Password Policy

New SOP

RCRV-CI-SOP-1.8
Secure use of RCRV
802.11 Wireless Networks

Appendix A
Documentation of
STIG Compliance

SOP Implementation
Example- 4.3: Training



Pre-Delivery Support:
- Provide CI trainings as a component

Post-Delivery Support:
-Provide additional CI trainings

Near Term:
- Work with OI Marine & Technical Groups develop training program

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

How this can impact you

- Hopefully help you streamline your SOP creation
- Implementing Best Practices = Improved security posture
- Plan to publish SOPs
  - Looking for feedback