Naval Facilities Engineering Systems Command

NAVFAC SOUTHEAST

Cybersecurity
Red Zone Commissioning for Design & Construction Projects

Presented by: Joseph Ellis

Panel: Andrea Freeman, Antonio Jefferson, Keith Long

09 December 2024

CIO Cybersecurity POCs

CYBERSECURITY PROGRAM OVERSIGHT

CIO2 CYBERSECURITY

CIO2: Joseph Ellis
Cybersecurity Division Director
904-542-5839

CIO21: Maria Lopez
RMF Team Lead
Risk Management Framework (RMF)
Requests for Authority-to-Operate (ATO)
904-546-9060

CIO42: Bobby Kelley
Control Systems Support Branch Manager
AMI, SCADA, DDC, and HVAC Support
Cyber Hygiene & Continuous Monitoring Support
904-542-2490

CIO: Andrea Freeman
Command Information Officer
904-542-4191

CIOPM: Antonio Jefferson
Cybersecurity Program Manager
Red Zone/Cybersecurity Commissioning
Construction and Design Contracts Review
904-546-9056

CIO43: Paddy Jackson
Information Systems Security Engineer Team Lead
Cybersecurity Commissioning Support
Risk Management Framework (RMF) Support
904-542-5488

CIO4 OPERATIONAL TECHNOLOGY

CIO4: Kevin Gaddist
Acting Operation Technology Division Director
904-542-8495

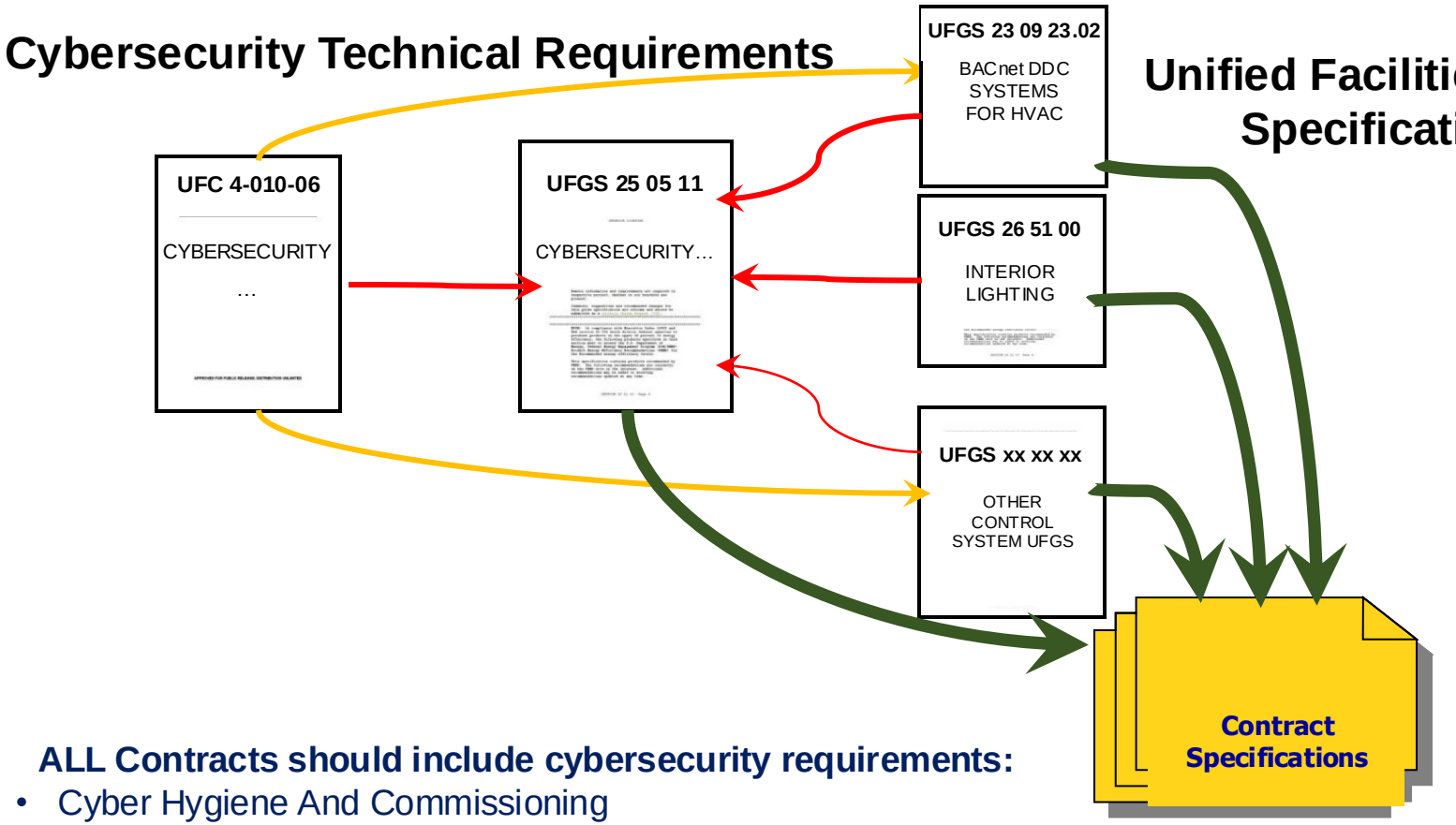
CIOC2: Joseph Ellis
Defensive Cybersecurity Operations
Protect Systems and Networks from Cyber Threats
Analyze Cyber Threats and Vulnerabilities
904-542-5839

CIO44: Keith Long
CyCx Team Lead
Cybersecurity Commissioning Support
Construction and Design Contracts Review
904-542-8434

Cybersecurity Red Zone Commissioning for Design & Construction Projects

- **UFC 4-10-06** establishes the criteria to ensure delivery of a secure Facility Related Control System (FRCS) while meeting facility operational requirements
- **UFGS 25 05 11** outlines cybersecurity requirements specifically for "Facility-Related Control Systems" (FRCS), essentially dictating how these systems should be designed and secured against cyber threats.
- **Red Zone Commissioning** evaluates implementation of the UFGS 25-05-11 and overall compliance with UFC 4-10-06
- NAVFAC SE designed and utilizes a FRCS Cybersecurity Commissioning **(CyCx) Checklist** derived from the UFGS 25-05-11 to track implementation for each identified FRCS.
- NAVFAC SE created and provides a **Close Out Memorandum** to the System Owner, for inclusion with the Acceptance Testing Results, that (1) addresses FRCS concerns related to residual risk and completion of commissioning; and (2) Informs the System Owner of overall cybersecurity compliance prior to beneficial occupancy date (BOD).

Cybersecurity For Facility-Related Control Systems

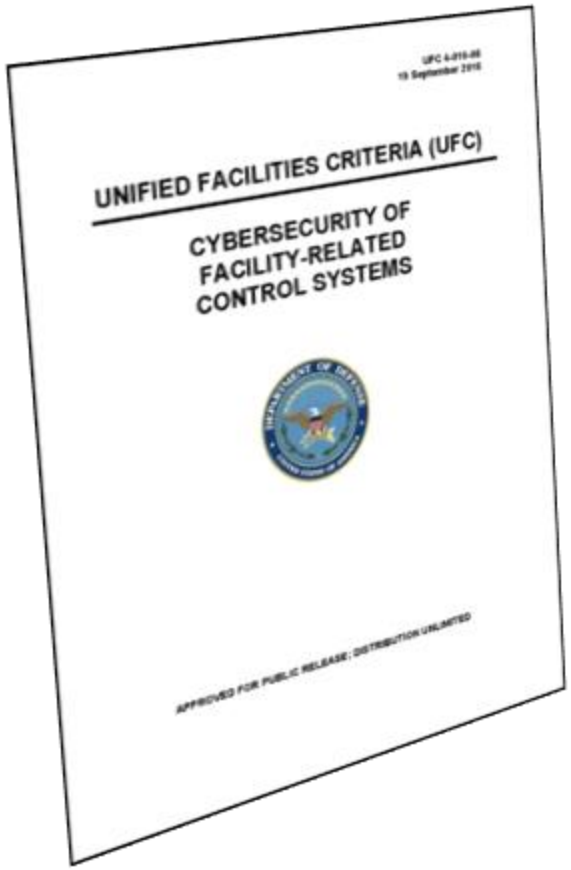


ALL Contracts should include cybersecurity requirements:

- Cyber Hygiene And Commissioning
- Contract Specifications With Cyber Criteria
- Government Representative From A CIO Department/Organization

Cybersecurity Criteria Should Be Included In Contract Specifications

Cybersecurity of Facility Related Control Systems: UFC 4-010-06



UPDATE PUBLISHED OCTOBER 2023

Unified Facilities Criteria (UFC)

- Provides planning, design, construction, sustainment, restoration, and modernization criteria.
- Applies to the Military Departments, the Defense Agencies, and the DoD Field Activities
- Used for all DoD projects and work for other customers where appropriate

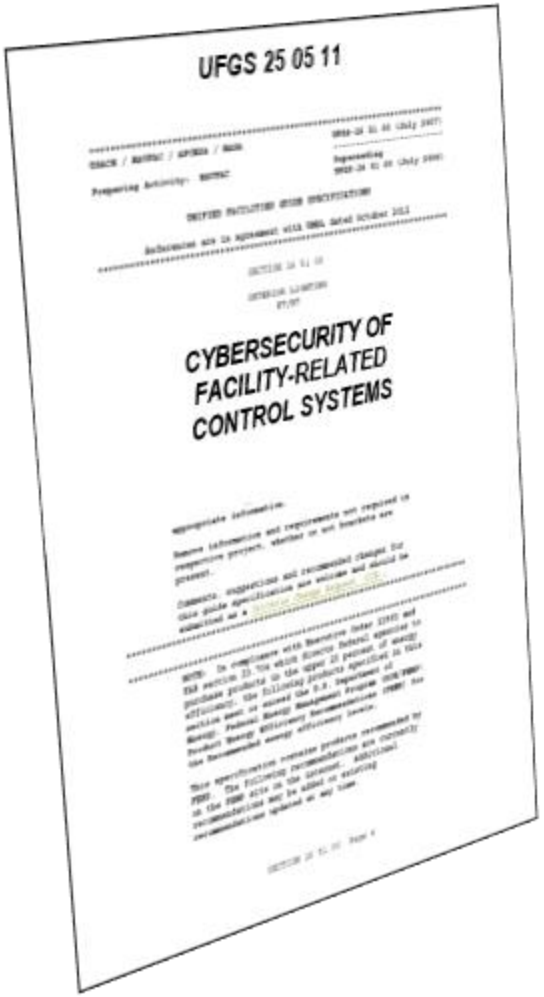
- **Integrates only a subset of Risk Management Framework (RMF) requirements for facility-related control systems**
- **Applies to all new construction and repair projects**
- **Narrows RMF Focus to design only and not system life cycle**
- **4-010-06 provides:**
  - Guidance to Designers-of-Record
  - Information intended for Designers-of-Record
  - Cyber Impact Levels of Confidentiality, Integrity, & Availability (C-I-A) Guidance for impact rating
  - Detailed guidance for LOW and MODERATE impact systems

5 Steps for Cybersecurity Design: UFC 4-010-06

- **Step 1:** Identify the Confidentiality, Integrity, and Availability (C-I-A) impact levels (LOW, MODERATE, or HIGH) to use for the control system design.
- **Step 2A:** Use the impact levels to select the proper list of controls from NIST SP 800-82.
- **Step 2B:** Create a list of relevant Control Correlation Identifiers (CCIs) based on the controls selected in Step 2A using the DoD master CCI list.
- **Step 2C:** Categorize CCIs and identify CCIs that require input from the designer or are the designer's responsibility.
- **Step 3:** Include cybersecurity requirements in the project specifications and provide input to others as required.

*****Design should not proceed without the proper C-I-A Impact ratings*****

Cybersecurity of Facility Related Control Systems: UFGS 25 05 11


UFGS 25 05 11

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

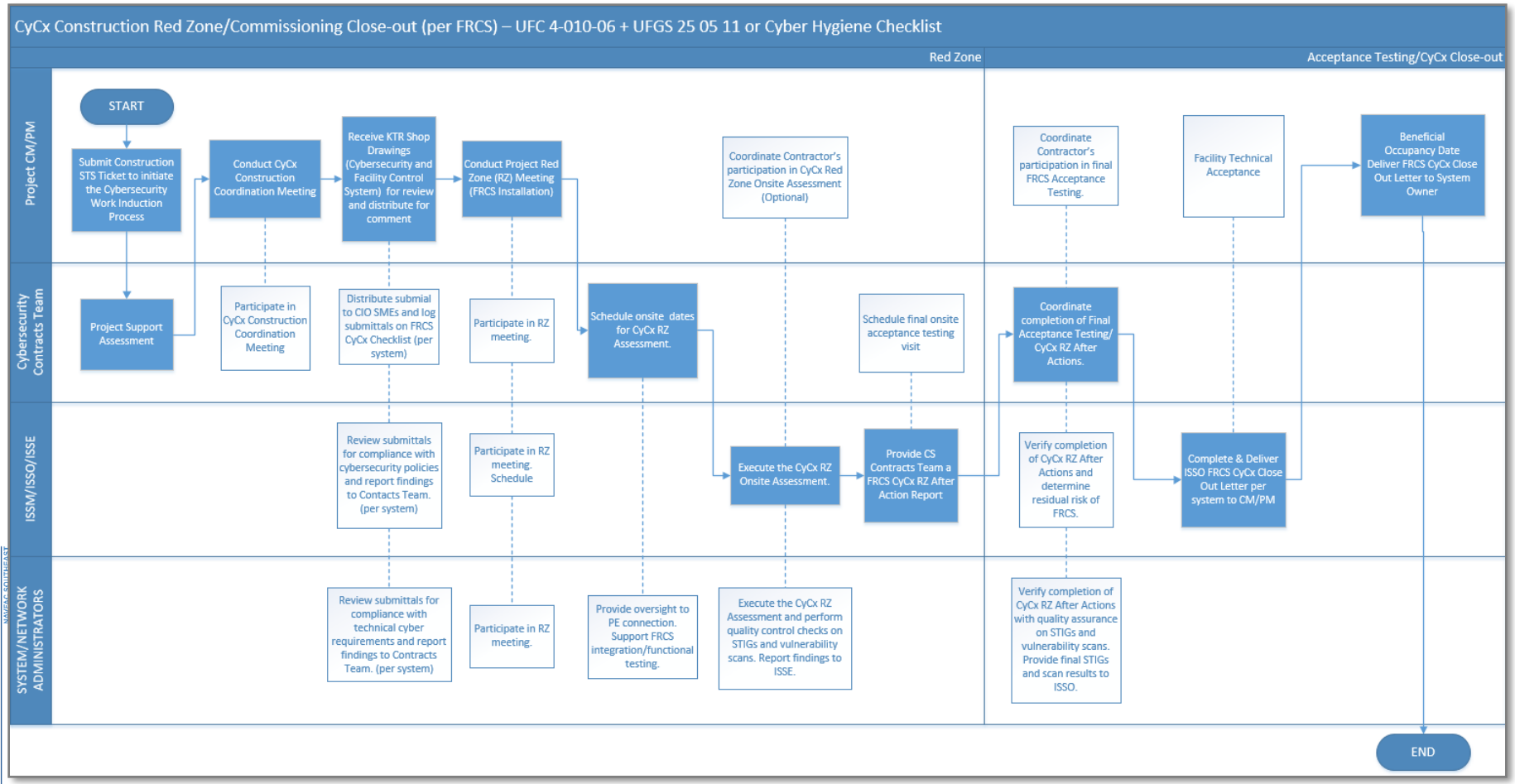
UPDATE REVISION PUBLISHED AUGUST 2024

- Whole Building Design Guide (www.wbdg.org)
- Consolidates all cybersecurity submittals into one specification
- Includes requirements to submit for contractual fulfillment by implementing cybersecurity into facility related controlled systems construction projects
- Requires security control submittals to be properly answered

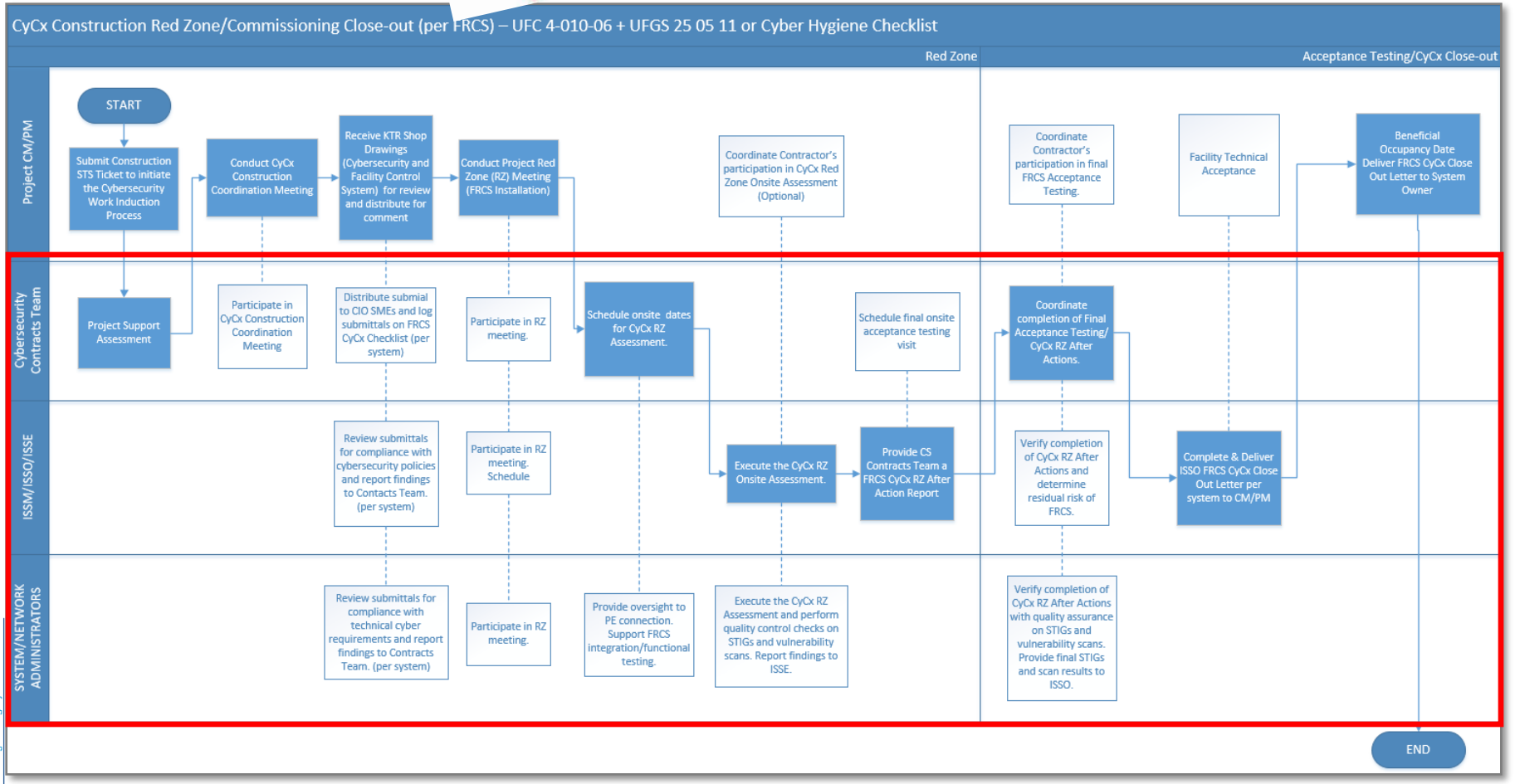
Design to Construction Transition

- **CIO involvement at the construction kick-off meeting and follow-on project status meetings is crucial**
  - Validates a UFGS 25-05-11 has been properly developed for each FRCS during design phase
  - Generates FRCS CyCx checklists for each UFGS 25-05-11 and provides data to the construction team
- **Change Management throughout the project is necessary to ensure FRCS are evaluated appropriately at Red Zone and Commissioning**
  - Ensures appropriate hardware and software is delivered
  - Simplifies inventory management at project completion

RED ZONE Commissioning Process



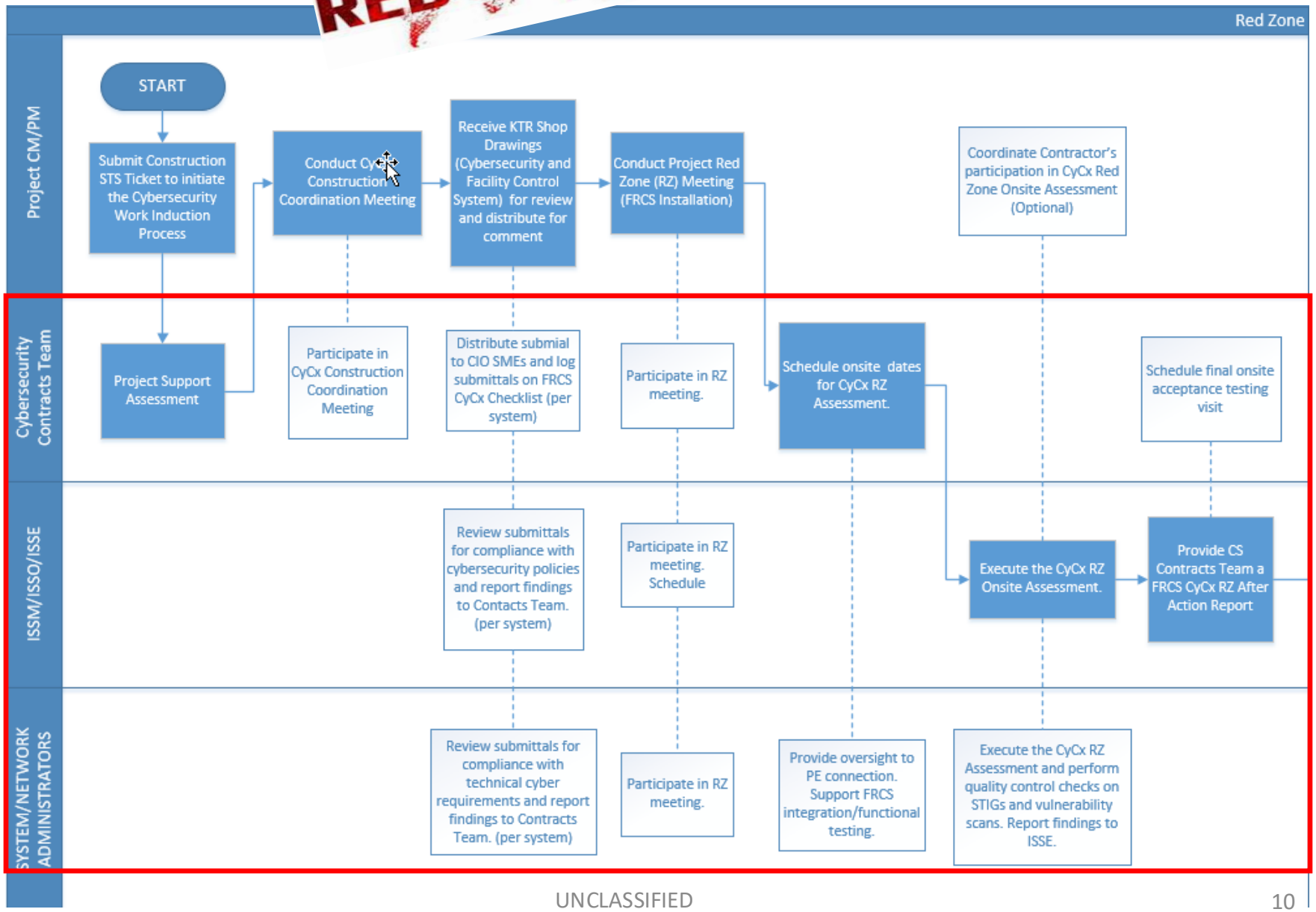
Cybersecurity RED ZONE Commissioning Process



- NAVFAC SE utilizes a FRCS Cybersecurity Commissioning (CyCx) Checklist derived from the UFGS 25-05-11 for each identified FRCS to track implementation

- System Owner receives a Close Out Memorandum at the end of the project outlining the overall cybersecurity compliance state for each FRCS

Pre-RED ZONE Action Items



FRCS CyCx Checklist

- Workbook consisting of:
  - Instruction/Data Dictionary
  - CyCx Checklist Data
  - Submittal Requirements
  - Red Zone After Action Report
- Created based on the NAVFAC Cyber Hygiene Checklists
- Provides a technical snapshot of the FRCS cybersecurity readiness status

NAVFAC FRCS Cybersecurity Commissioning (CyCx) Checklist

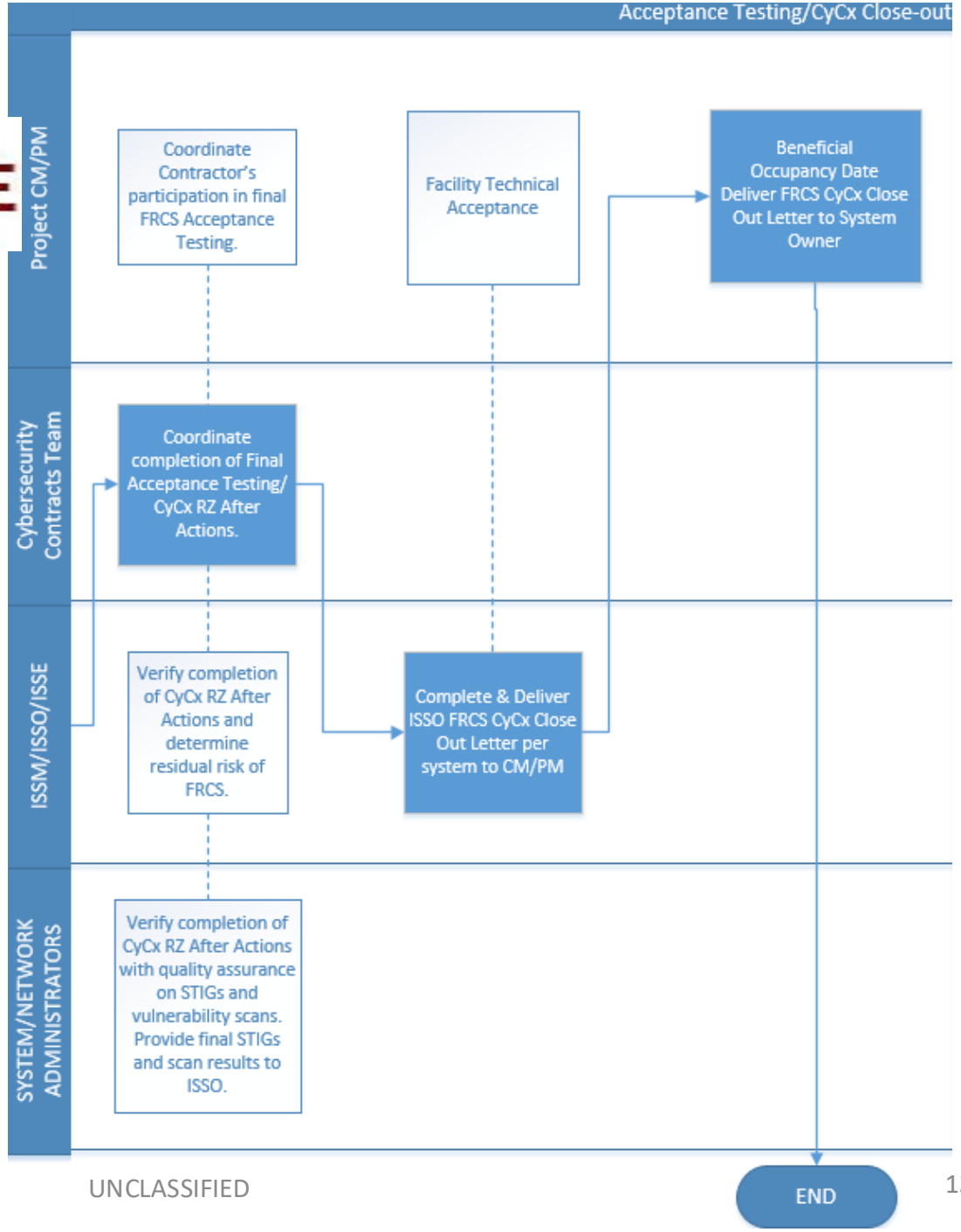
Project or Work Order Number:	
Control System or Device/Component (Choose one):	
Control System or Device/Component Name:	
Date:	

Read instruction tab before completing this checklist. Contractor is to complete this checklist for each control system and/or component. These devices will range between Levels 2 - 5 of the UFC 04-01-06 Control System Architecture. ***NOTE: If each device type is identical and configured the same, only one sheet required.***

Task ID	Requirement	Reference	Status	Comments
	Contractor/Vendor			
C1	Have all unused accounts been deleted from control system?	AC-2		
C2	Have all shared credentials/accounts utilized on the control system been approved by the government. If not, provide explanation in the comments.	AC-2		
C3	Have all control system accounts been modified to the concept of least privileged; leaving only authorized user and services access required to meet the mission of the system?	AC-6		
C4	Are there user initiated methods and/or mechanism to prevent unauthorized access to the control system when left unattended?	AC-11		
C5	Has all remote access been approved by the government?	AC-17		
C6	Are all control system wireless network access configured with to the DoD approved encryption standards? If not, provide explanation in comments?	AC-18		
C7	Have control system logs have been reviewed and appropriate actions taken based on log content (i.e. alarms)?	AU-1		
C8	Has the inventory of all physical devices and systems been documented on a control system inventory and approved by the government?	CM-8		
C9	Has the inventory of all software and software licenses been documented and approved by the government?	CM-8		
C10	Have all default passwords been changed to meet the DoD password standards or set to the maximum strength allowable by the operating system or firmware?	IA-5		
C11	Are all physical access points to the control system and its components installed where monitored physical access authorization controls are in place (i.e., CCTV, alarms, guards) or is properly secured (i.e., behind a locked door or enclosure)? If not, provide explanation in comments.	PE-3, PE-6		
C12	Does the control system have long-term alternate power supply in the event of an extended loss of the primary power source?	PE-11		
C13	Have all control system parts and replacement components been verified as genuine and not been altered?	SA-12		
C14	Has government approved installation of any components and software approaching or at end of life support?	SA-22		
C15	Does the control system fail to a secure state in an event of a failure during system initialization, shutdown, and aborts?	SC-24		
C16	Are all non-essential or unrequested functionalities, connection ports and input/output devices physically disabled or removed?	SC-41		
	Government Use Only			
G1	All privilege user have an approved Navy System Access Authorization Request (SAAR-N) on file documenting a proper background investigation and completed privileged access agreement?	AC-6(5)		
G2	All operator/technician(s) have an approved Navy System Access Authorization Request (SAAR-N) on file documenting completion of annual Cyber Awareness Training.	AT-2		
G3	Has a Continuous Monitoring plan been documented, and if so, has that Plan been implemented which focuses on, at a minimum, the following core tasks: POA&M updates, patching, reporting, configuration management (CM), log file analysis, account management, firmware updates? (To include scanning when possible/applicable)	CA-7		
G4	Have the operator/technician(s) been informed that changes to the control system baseline may have a cybersecurity impact and require coordination with CIO/N6/System Owner.	CM-2		
G5	Has the Incident Response Plan (IRP) applicable to this control system been updated for any unique requirements associated with this control system? If so, provide explanation in the comments.	IR-1		
G6	Has the Physical Security Officer and after-hours point of contract of the control system space been documented? If not, document in the comments.	MA-5		

RED ZONE

Commissioning Closeout



FRCS CyCx Checklist Example: Control Implementation Assessment

NAVFAC FRCS Cybersecurity Commissioning (CyCx) Checklist	
Project or Work Order Number:	**P426**
Control System or Device/Component (Choose one):	**Control System**
Control System or Device/Component Name:	**LCS Facility DDC**
Date:	**Monday, May 16, 2022**

Read instruction tab before completing this checklist. Contractor is to complete this checklist for each control system and/or component. These devices will range between Levels 2 - 5 of the UFC 04-01-06 Control System Architecture. ***NOTE: If each device type is identical and configured the same, only one sheet required.***

Task ID	Requirement	Reference	Status	Comments
	Contractor/Vendor			
C1	Have all unused accounts been deleted from control system?	AC-2	Compliant	No unused account present.
C2	Have all shared credentials/accounts utilized on the control system been approved by the government. If not, provide explanation in the comments.	AC-2	Compliant	There are no shared accounts associated with the system
C3	Have all control system accounts been modified to the concept of least privileged; leaving only authorized user and services access required to meet the mission of the system?	AC-6	Compliant	At this time there are only one account for administrative purposes
C4	Are there user initiated methods and/or mechanism to prevent unauthorized access to the control system when left unattended?	AC-11	Not Applicable	Requirement will be re-assessed for update to checklist.
C5	Has all remote access been approved by the government?	AC-17	Compliant	There is remote access connectivity
C6	Are all control system wireless network access configured with to the DoD approved encryption standards? If not, provide explanation in comments?	AC-18	Not Applicable	Wireless mechanism will be physically removed from JACE.
C7	Have control system logs have been reviewed and appropriate actions taken based on log content (i.e. alarms)?	AU-1	Not Applicable	N/A at this time until fully operational
C8	Has the inventory of all physical devices and systems been documented on a control system inventory and approved by the government?	CM-8	Compliant	
C9	Has the inventory of all software and software licenses been documented and approved by the government?	CM-8	Compliant	
C10	Have all default passwords been changed to meet the DoD password standards or set to the maximum strength allowable by the operating system or firmware?	IA-5	Not Applicable	At this time this security controls has not been implemented until full turnover.
C11	Are all physical access points to the control system and its components installed where monitored physical access authorization controls are in place (i.e., CCTV, alarms, guards) or is properly secured (i.e., behind a locked door or enclosure)? If not, provide explanation in comments.	PE-3, PE-6	Compliant	CAC enabled readers for door locks are installed throughout the facility
C12	Does the control system have long-term alternate power supply in the event of an extended loss of the primary power source?	PE-11	Not Applicable	CIO will determine if building generator will power building PLCs and other level 0 and 1 device.

FRCS CyCx Checklist Example: Submittals

NAVFAC FRCS Cybersecurity Commissioning (CyCx) Checklist Other Requirements				
Project or Work Order Number:	**P426 LITTORAL COMBAT SHIP (LCS) SUPPORT FACILITY MAYPORT CONTRACT: N69450-19-C-0913**			
Control System or Device/Component (Choose one):	**Control System**			
Control System or Device/Component Name:	**P426 LITTORAL COMBAT SHIP (LCS) Direct Digital Control**			
Contractor is to complete this checklist for all FRCS associated with the project, reference the instructions tab for guidance.				
Task ID	**Requirement**	**Affected CCI / AP**	**Status**	**Comments**
SD-01 Preconstruction Submittals				
1	Wireless and Wired Broadcast Communication Request	AC-18	Not Submitted	**Updated 7/26/22: Initially marked NA due the contractor reporting no wireless communications requirement (See Submittal 347.02-25 05 11). Wireless communication was recently discovered. Gov't will remediate after BOD.** Physical device will be removed.
2	Device Account Lock Exception Request	AC-7	Not Applicable	Not Applicable
3	Multiple Ethernet Connection Device Request	PL-8	Not Applicable	Not Applicable
4	Contractor Computer Cybersecurity Compliance Statements	PL-4	Approved	
5	Contractor Temporary Network Cybersecurity Compliance Statements	PL-4	Approved	
6	Cybersecurity Interconnection Schedule	PL-8	Approved	**Updated 7/26/22: Contractor provided submittal on 7/14/22. Wireless communication was not identified on schedule.** Awaiting attachment 1 as stated on front page of submittal package dated 4/12/22.
7	Protection of Information At Rest Proposal	SC-28	Not Applicable	Out of scope for UFGS 25 05 11 spec only. Contractor is directed to follow other specifications related to this topic.
8	Proposed STIG and SRG Applicability Report	CM-2	Not Applicable	Out of scope for UFGS 25 05 11 spec only. Contractor is directed to follow other specifications related to this topic.
SD-02 Shop Drawings				
1	Network Communication Report	CA-9, CM-6, CM-7, PL-8, SC-8, SC-41	Approved	**Updated 7/26/22: Contractor provided submittal on 7/14/22. Information provided with the Cybersecurity Interconnection Schedule documents additional information needed for this report. Wireless communication was not identified in report. Wireless capability was reported as no requirement. (See Submittal 347.02-25 05 11).** Contractor stated "Will Submit Later" on submittal package dated 4/12/22.

FRCS CyCx Checklist Example: Red Zone After Action Report

NAVFAC FRCS Cybersecurity Commissioning (CyCx) Checklist
Red Zone after Action Report
(For Government Use Only)

Project or Work Order Number:	**P426**
Control System or Device/Component (Choose one):	**Control System**
Control System or Device/Component Name:	**LCS Facility DDC**
Date:	**Friday, May 20, 2022**

Contractor and government are required to completed listed actions. NAVFAC SE CIO ISSE will document validation of completed and not completed actions on this report. Actions not completed will be listed on the Cybersecurity Commissioning (CyCx) Closeout memo.

Noteworthy Strengths

1	Collaboration between LCSRON 2, PWD Mayport, Walsh Group and Johnson Control.
2	Lock down of physical access points to the control system.
3	Chris (Johnson Controls) Control System subject matter expert (SME) knowledge of cybersecurity
4	Maria Santos, Construction Manager, use of Flank Speed Tools for team collaboration (i.e., meetings,
5	Joshua Fowler asking questions based on lessons learned with turning over systems to the BOSC.

Task ID	Action	Comments	ISSE's Validation
Contractor After-Actions			
CA1	Physically disable the wireless device on the JACE located in the 1st floor mechanical room.	Wireless communication was recently discovered. Only the wireless capabilities has been disable. Gov't will remediate after BOD.	Validation completed 7/26/22 by LouShawda Grant, 904-542-8404
CA2	Submit remaining submittals listed on the 'Submittal" tab. These submittals were expected at a later date as stated on transmittal #347 dated 4/13/2022.	Remaining submittals submitted and approved.	Validation completed 7/26/22 by LouShawda Grant, 904-542-8404
Government After-Actions			
GA1	NAVFAC SE CIO4 provide STIG training to Welsh Group and Johnson controls.	Bobby Kelly completed training on 7/25/22.	Validation completed 7/26/22 by LouShawda Grant, 904-542-8404
GA2	NAVFAC SE CIO4 perform baseline scanning.	Bobby Kelly completed scanning. Results are at M:\CIO\CIO_2\ISSE\Mayport_P426_documents.	Validation completed 7/26/22 by LouShawda Grant, 904-542-8404
GA3	NAVFAC SE CIO4 provide DoD User Banner application training to Welsh Group and Johnson controls.	Bobby Kelly completed training on 7/25/22.	Validation completed 7/26/22 by LouShawda Grant, 904-542-8404
GA4	PWD Mayport locate transmittal #347 attachment 1. Attachment 1 was submitted as the Cybersecurity Interconnection Schedule.	Submitted and approved	Validation completed 7/26/22 by LouShawda Grant, 904-542-8404
GA5	PWD Mayport schedule and communicate turnover date for DDC equipment.	Turnover date is set for 7/29/22. Laptop turned over on 6/27/22 to Joshua Fowler	Validation completed 7/26/22 by LouShawda Grant, 904-542-8404

CyCx Closeout Memorandum

- Provided to the System Owner and Construction Manager for inclusion in the Acceptance Testing Results
  - Addresses FRCS concerns related to residual risk and completion of commissioning
  - Informs the System Owner of overall cybersecurity compliance prior to beneficial occupancy date (BOD)

29 Jul 22

MEMORANDUM

From: NAVFAC Southeast Operational Technology Information System Security Manager

To: Public Works Officer Mayport

Subj: Cybersecurity Commissioning (CyCx) Closeout of Direct Digital Control (DDC) System of Contract #N69450-19-C-0913 P426 LITTORAL COMBAT SHIP (LCS) SUPPORT FACILITY MAYPORT

Encl: (1) P426 LITTORAL COMBAT SHIP (LCS) FRCS Cybersecurity Commissioning Checklist

1. The DDC commissioned under the subject construction contract has been accepted by the Command Information Office (CIO) as of the Building Occupancy Date (BOD) of 30 July 2022. Approval representatives for the final commissioning validation:

   a. LouShawda Grant, Cyber Design & CyCx SME, NAVFAC Southeast CIO2

   b. Bobby Kelley, CyCx Technical Validator, NAVFAC Southeast CIO4

2. Enclosure (1) contains the Red Zone after Action Report final validation results of the Cybersecurity FRCS commissioning efforts in support of P426 LCS Support Facility.

3. During the cybersecurity commissioning validation review visit, active wireless communication was discovered. To minimize the risk, the wireless capabilities have been disabled. Government will assess the DDC's dependency on wireless communication after BOD.

4. Overall Cybersecurity compliance of the DDC is acceptable and meets the minimum requirement for integration into the base wide DDC boundary.

A. Jefferson

Questions?