NAVFAC
Naval Facilities Engineering Systems Command
NAVFAC SOUTHEAST

Red Zone Cybersecurity Commissioning
for Design & Construction Projects

Presented by: Nate McCarty

Panel: Antonio Jefferson, Joe Ellis, Charlie Weaver & Kevin Gaddist

11 Jan 2024

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

CIO Cybersecurity POCs

CYBERSECURITY PROGRAM OVERSIGHT

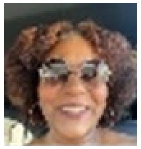
CIO2 CYBERSECURITY

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

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

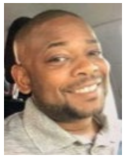
CIO4 OPERATIONAL TECHNOLOGY

CIO4: Charlie Weaver - 904-542-8482
Operational Technology Division Director



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

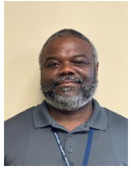
CIOPM: Antonio Jefferson - 904-546-9056
Cybersecurity Contracts Program Manager
Red Zone Commissioning and BOD Support
Construction and Design Contracts Review



CIO41: Kevin Gaddist - 904-542-8495
OT Enterprise Support Branch Manager
Control System Platform Enclave (CSPE)
Continuous Monitoring Support

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

CIO43: Paddy Jackson - 904-542-1384
Information Systems Security Engineer Team Lead
Cybersecurity Commissioning Support
Risk Management Framework (RMF) Support



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

Red Zone Cybersecurity Commissioning for Design & Construction Projects

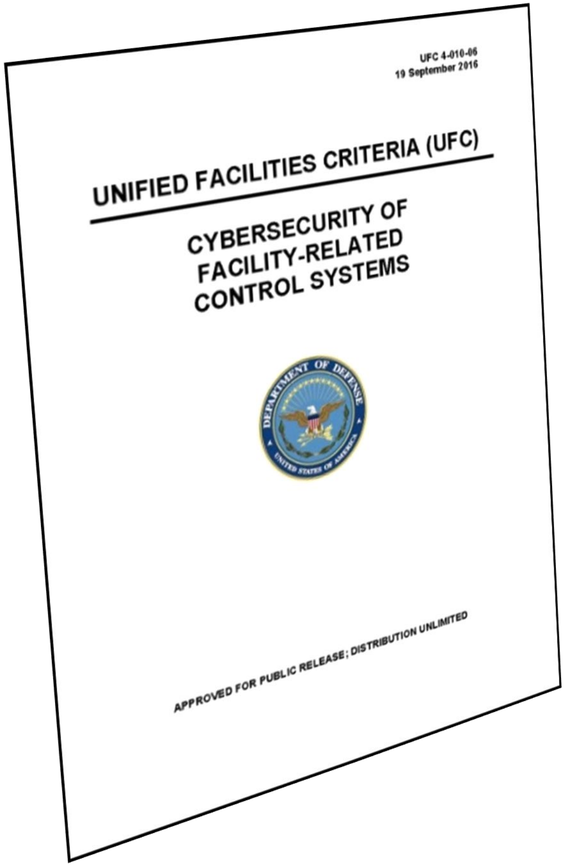
Red Zone Cybersecurity Commissioning (CyCx) is a method of evaluating whether the cybersecurity controls applied to a Facility Related Control System (FRCS) meet contract requirements using UFC and UFGS guides.

- **UFC 4-10-06** Cybersecurity for Facility Related Control System (FRCS)

- **UFGS 25-05-11** Guide Specification for Cybersecurity for FRCS

NAVFAC SE developed a **FRCS Cybersecurity Commissioning (CyCx) Checklist** derived from the UFGS 25-05-11 to track contract compliance.

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



UFC 4-010-06
19 September 2016

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF
FACILITY-RELATED
CONTROL SYSTEMS

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

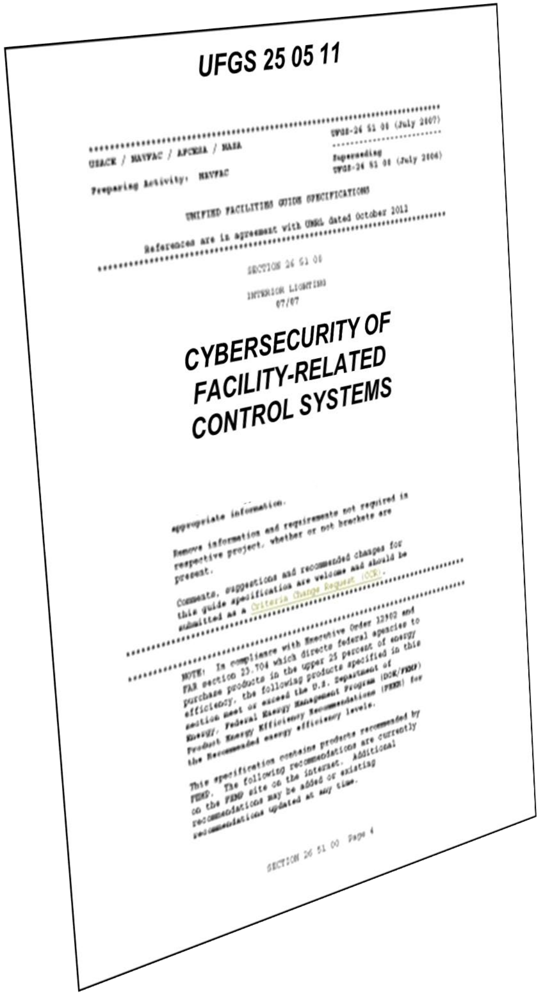
Update published 10-October-2023

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

Cybersecurity of Facility Related Control Systems: UFGS 25 05 11



UFGS 25 05 11

USACE / NAVFAC / AFCESA / NASA

UFGS-26 51 00 (July 2007)

Superseding
UFGS-26 51 00 (July 2006)

Preparing Activity: NAVFAC

UNIFIED FACILITIES GUIDE SPECIFICATIONS

References are in agreement with UMRL dated October 2012

SECTION 26 51 00

INTERIOR LIGHTING
07/07

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

appropriate information.

Remove information and requirements not required in respective project, whether or not brackets are present.

Comments, suggestions and recommended changes for this guide specification are welcome and should be submitted as a Criteria Change Request (CCR).

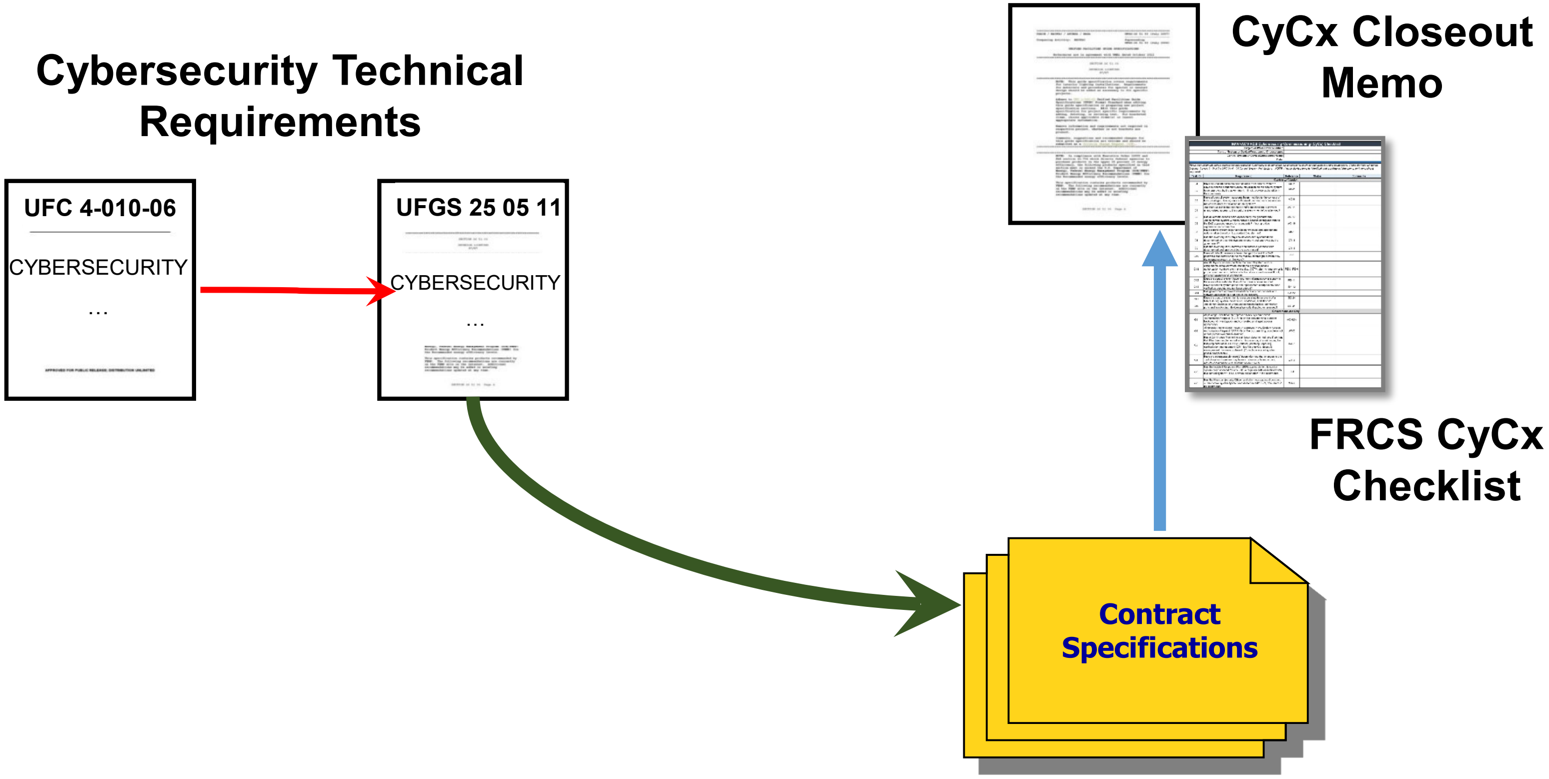
NOTE: In compliance with Executive Order 13702 and FAR section 23.704 which directs federal agencies to purchase products in the upper 25 percent of energy efficiency, the following products specified in this section meet or exceed the U.S. Department of Energy, Federal Energy Management Program (DOE/FEMP) Product Energy Efficiency Recommendations (PEER) for the Recommended energy efficiency levels.

This specification contains products recommended by FEMP. The following recommendations are currently on the FEMP site on the internet. Additional recommendations may be added or existing recommendations updated at any time.

SECTION 26 51 00 Page 4

- Update published August 2023
  - Whole Building Design Guide (www.wbdg.org)
- Consolidated 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

Red Zone Cybersecurity Commissioning For Facility-Related Control Systems



Cybersecurity Technical Requirements

UFC 4-010-06

CYBERSECURITY

…

UFGS 25 05 11

CYBERSECURITY

…

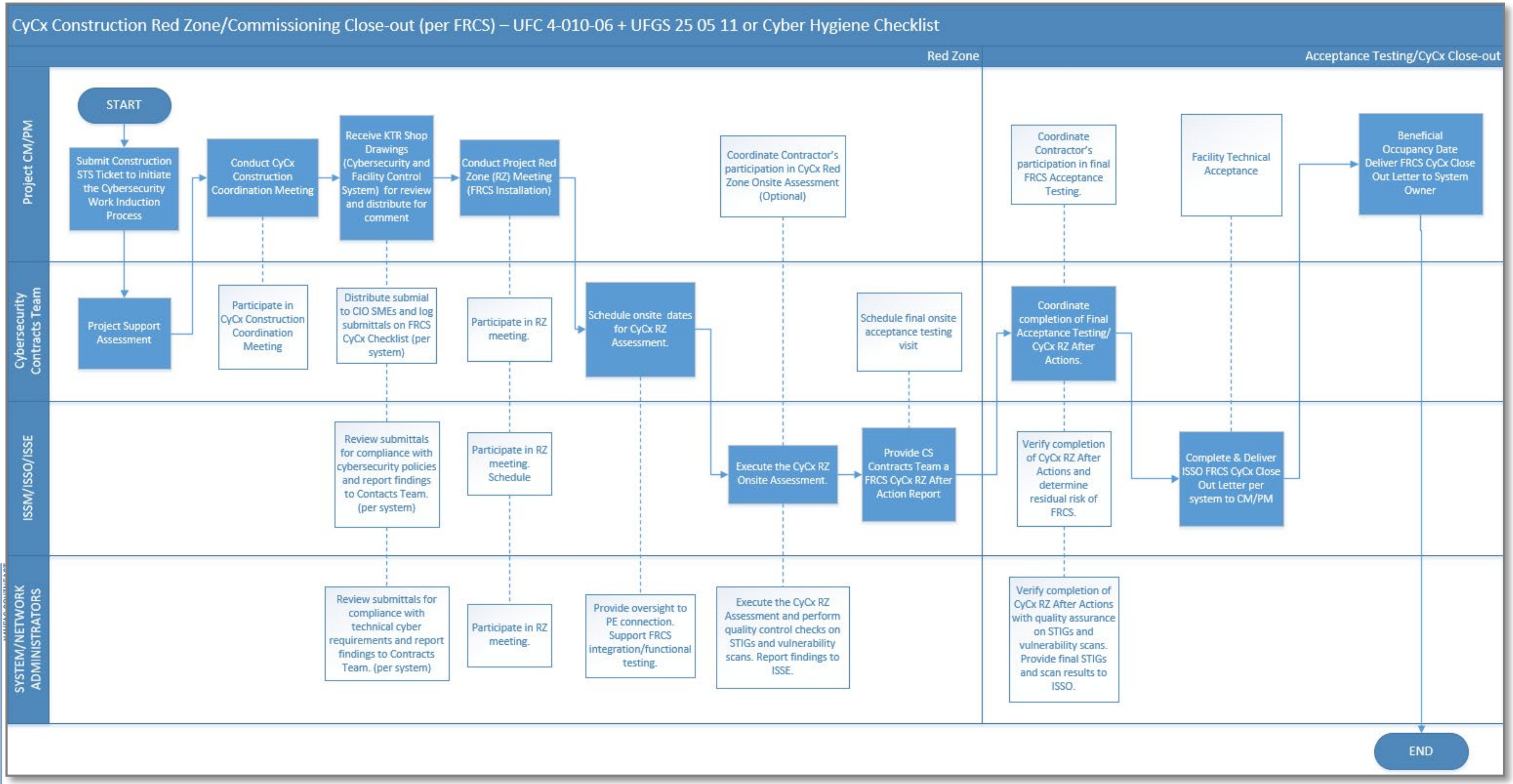
Contract Specifications

CyCx Closeout Memo

FRCS CyCx Checklist

Cybersecurity Criteria Should Be Included In Contract Specifications

Red Zone Commissioning Process



CyCx Construction Red Zone/Commissioning Close-out (per FRCS) – UFC 4-010-06 + UFGS 25 05 11 or Cyber Hygiene Checklist

Red Zone

Acceptance Testing/CyCx Close-out

Project CM/PM

START

Submit Construction STS Ticket to initiate the Cybersecurity Work Induction Process

Conduct CyCx Construction Coordination Meeting

Receive KTR Shop Drawings (Cybersecurity and Facility Control System) for review and distribute for comment

Conduct Project Red Zone (RZ) Meeting (FRCS Installation)

Coordinate Contractor's participation in CyCx Red Zone Onsite Assessment (Optional)

Coordinate Contractor's participation in final FRCS Acceptance Testing.

Facility Technical Acceptance

Beneficial Occupancy Date Deliver FRCS CyCx Close Out Letter to System Owner

Cybersecurity Contracts Team

Project Support Assessment

Participate in CyCx Construction Coordination Meeting

Distribute submial to CIO SMEs and log submittals on FRCS CyCx Checklist (per system)

Participate in RZ meeting.

Schedule onsite dates for CyCx RZ Assessment.

Schedule final onsite acceptance testing visit

Coordinate completion of Final Acceptance Testing/ CyCx RZ After Actions.

ISSM/ISSO/ISSE

Review submittals for compliance with cybersecurity policies and report findings to Contacts Team. (per system)

Participate in RZ meeting. Schedule

Execute the CyCx RZ Onsite Assessment.

Provide CS Contracts Team a FRCS CyCx RZ After Action Report

Verify completion of CyCx RZ After Actions and determine residual risk of FRCS.

Complete & Deliver ISSO FRCS CyCx Close Out Letter per system to CM/PM

SYSTEM/NETWORK ADMINISTRATORS

Review submittals for compliance with technical cyber requirements and report findings to Contracts Team. (per system)

Participate in RZ meeting.

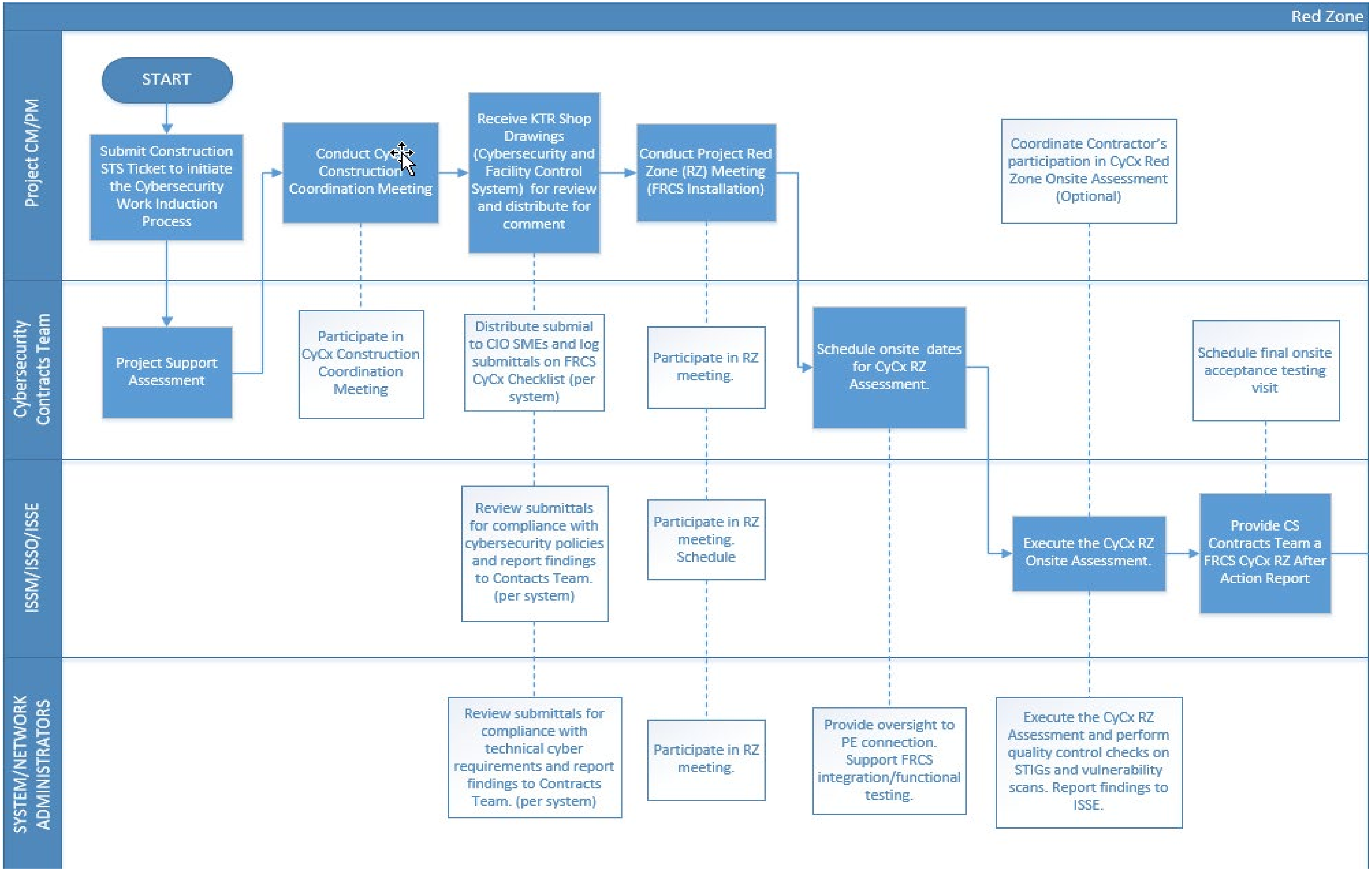
Provide oversight to PE connection. Support FRCS integration/functional testing.

Execute the CyCx RZ Assessment and perform quality control checks on STIGs and vulnerability scans. Report findings to ISSE.

Verify completion of CyCx RZ After Actions with quality assurance on STIGs and vulnerability scans. Provide final STIGs and scan results to ISSO.

END

Pre-Red Zone Commissioning Process



Red Zone

Project CM/PM

START

Submit Construction STS Ticket to initiate the Cybersecurity Work Induction Process

Conduct Cy[illegible] Construction Coordination Meeting

Receive KTR Shop Drawings (Cybersecurity and Facility Control System) for review and distribute for comment

Conduct Project Red Zone (RZ) Meeting (FRCS Installation)

Coordinate Contractor's participation in CyCx Red Zone Onsite Assessment (Optional)

Cybersecurity Contracts Team

Project Support Assessment

Participate in CyCx Construction Coordination Meeting

Distribute submial to CIO SMEs and log submittals on FRCS CyCx Checklist (per system)

Participate in RZ meeting.

Schedule onsite dates for CyCx RZ Assessment.

Schedule final onsite acceptance testing visit

ISSM/ISSO/ISSE

Review submittals for compliance with cybersecurity policies and report findings to Contacts Team. (per system)

Participate in RZ meeting. Schedule

Execute the CyCx RZ Onsite Assessment.

Provide CS Contracts Team a FRCS CyCx RZ After Action Report

SYSTEM/NETWORK ADMINISTRATORS

Review submittals for compliance with technical cyber requirements and report findings to Contracts Team. (per system)

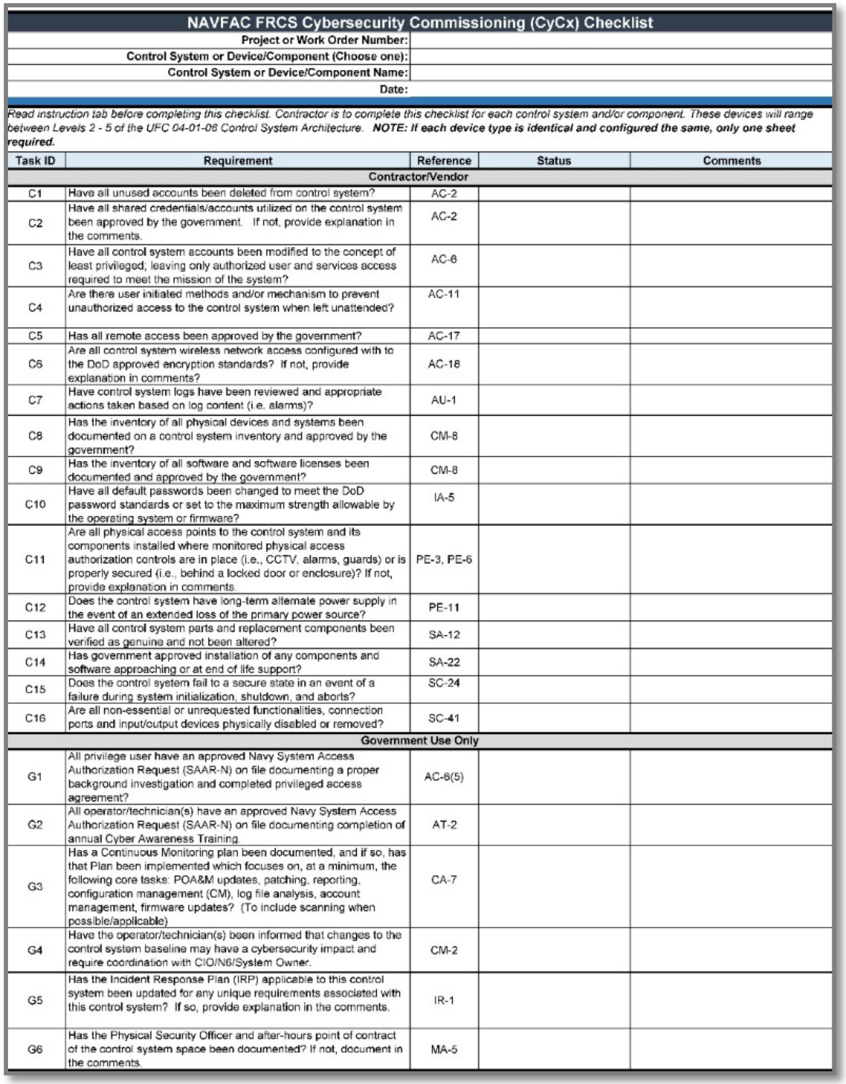
Participate in RZ meeting.

Provide oversight to PE connection. Support FRCS integration/functional testing.

Execute the CyCx RZ Assessment and perform quality control checks on STIGs and vulnerability scans. Report findings to ISSE.

NAVFAC FRCS CyCx Checklist

- Based on the UFGS 25-05-11
- A technical snapshot of the FRCS CS readiness status
- Workbook consists of:
  - Instructions
  - CyCx Checklist Data
  - Required Submittals
  - Red Zone After Action Report



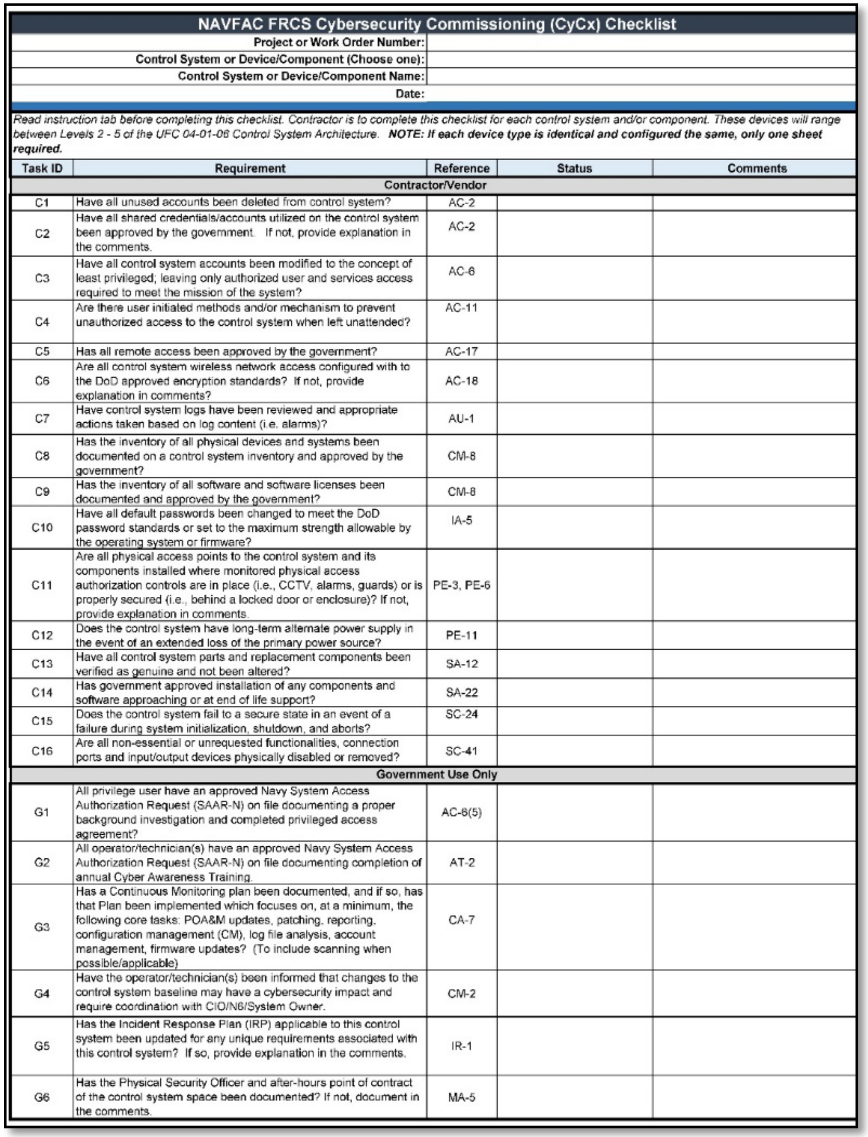
NAVFAC FRCS Cybersecurity Commissioning (CyCx) Checklist

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		

NAVFAC FRCS CyCx Checklist Example: Control Implementation Assessment

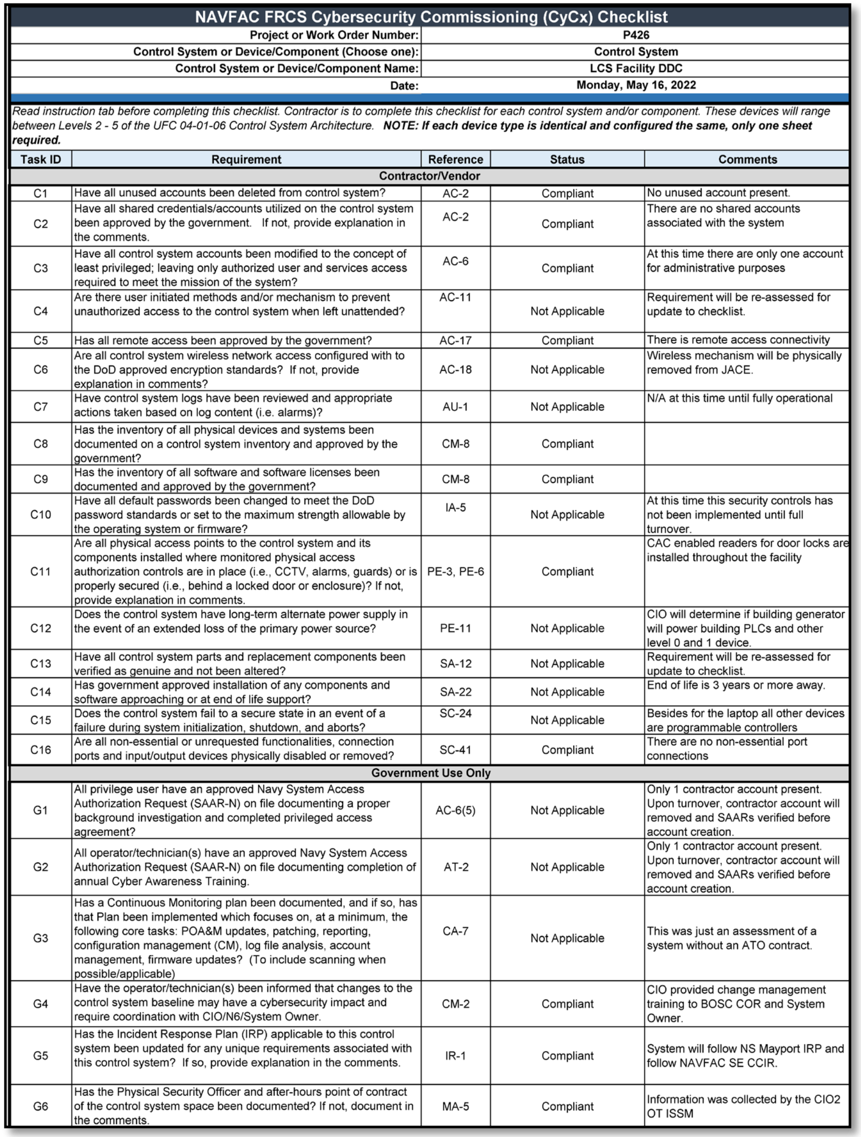


NAVFAC FRCS Cybersecurity Commissioning (CyCx) Checklist

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		



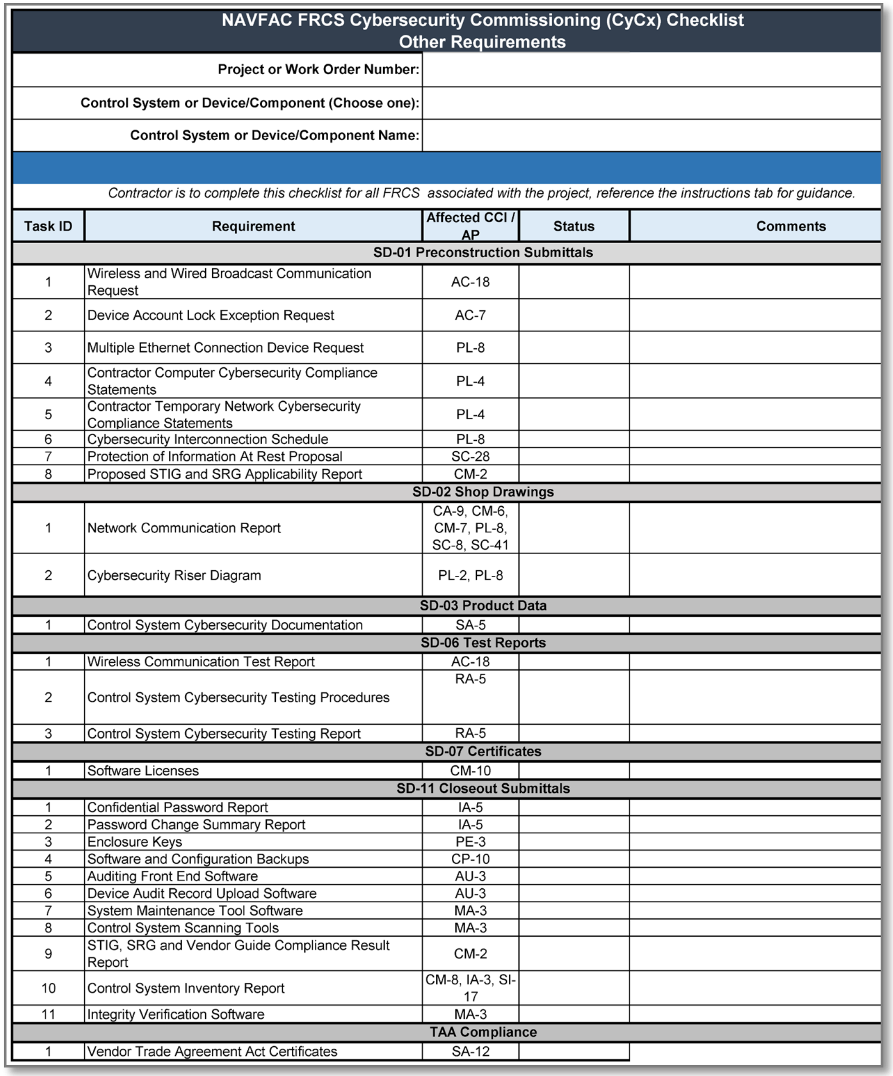
NAVFAC FRCS Cybersecurity Commissioning (CyCx) Checklist

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**

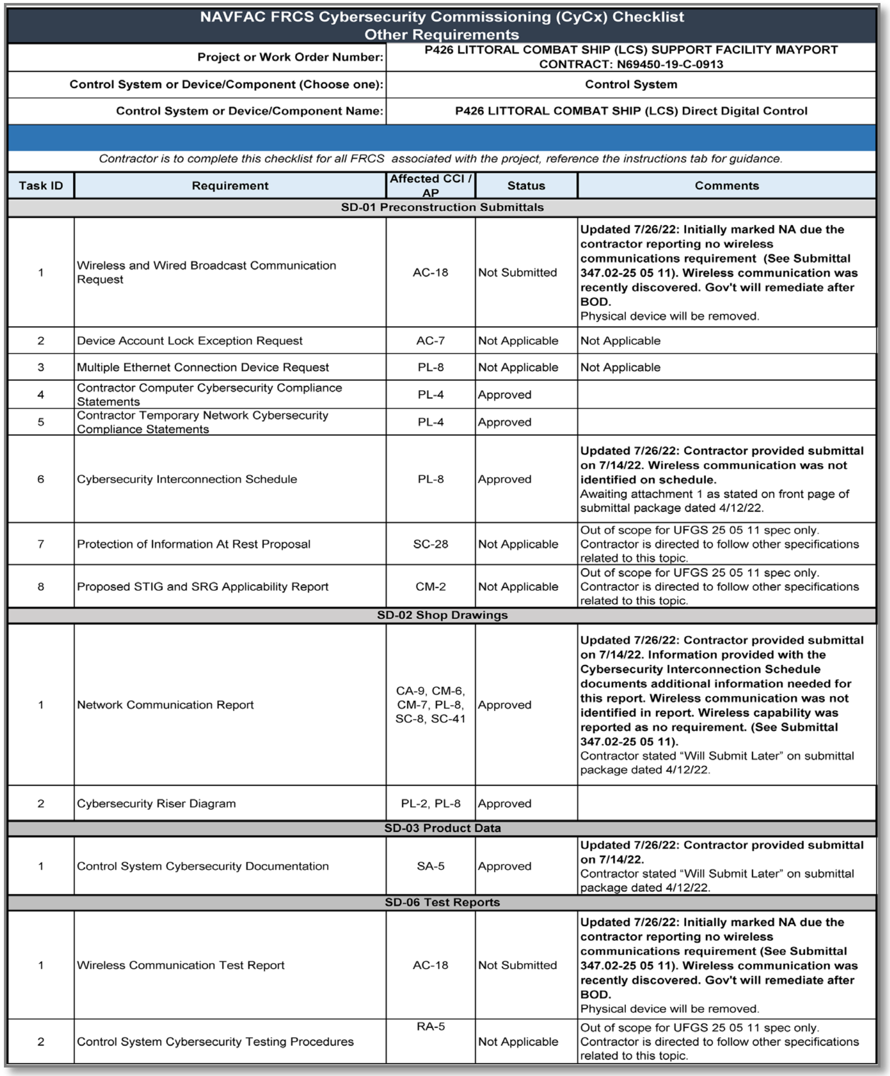
Read instruction tab before completing this checklist. Contractor is to complete this checklist for each control system and/or component. These devices will range between Levels 2 - 5 of the UFC 04-01-06 Control System Architecture. ***NOTE: If each device type is identical and configured the same, only 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.
C13	Have all control system parts and replacement components been verified as genuine and not been altered?	SA-12	Not Applicable	Requirement will be re-assessed for update to checklist.
C14	Has government approved installation of any components and software approaching or at end of life support?	SA-22	Not Applicable	End of life is 3 years or more away.
C15	Does the control system fail to a secure state in an event of a failure during system initialization, shutdown, and aborts?	SC-24	Not Applicable	Besides for the laptop all other devices are programmable controllers
C16	Are all non-essential or unrequested functionalities, connection ports and input/output devices physically disabled or removed?	SC-41	Compliant	There are no non-essential port connections
	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)	Not Applicable	Only 1 contractor account present. Upon turnover, contractor account will removed and SAARs verified before account creation.
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	Not Applicable	Only 1 contractor account present. Upon turnover, contractor account will removed and SAARs verified before account creation.
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	Not Applicable	This was just an assessment of a system without an ATO contract.
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	Compliant	CIO provided change management training to BOSC COR and System Owner.
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	Compliant	System will follow NS Mayport IRP and follow NAVFAC SE CCIR.
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	Compliant	Information was collected by the CIO2 OT ISSM

NAVFAC FRCS CyCx Checklist Example: Submittals

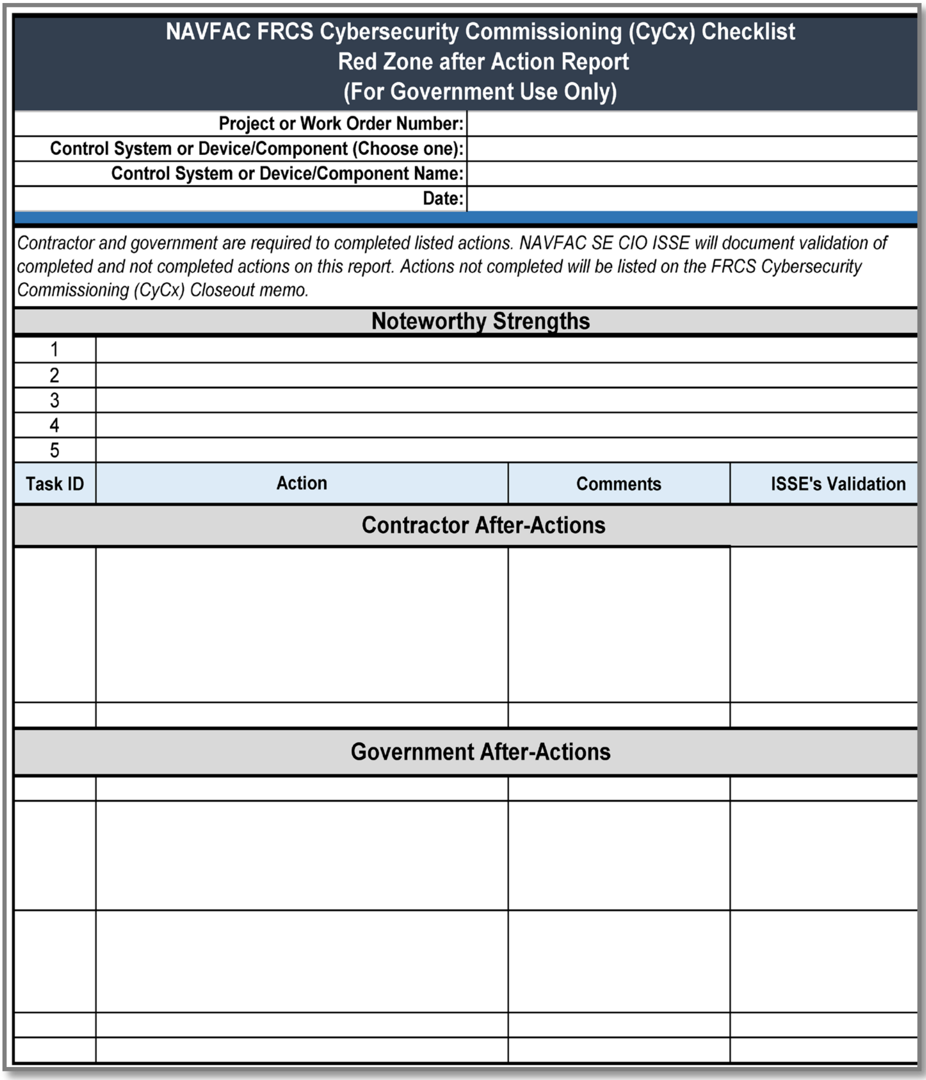


NAVFAC FRCS Cybersecurity Commissioning (CyCx) Checklist Other Requirements				
Project or Work Order Number:				
Control System or Device/Component (Choose one):				
Control System or Device/Component Name:				
Contractor is to complete this checklist for all FRCS associated with the project, reference 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		
2	Device Account Lock Exception Request	AC-7		
3	Multiple Ethernet Connection Device Request	PL-8		
4	Contractor Computer Cybersecurity Compliance Statements	PL-4		
5	Contractor Temporary Network Cybersecurity Compliance Statements	PL-4		
6	Cybersecurity Interconnection Schedule	PL-8		
7	Protection of Information At Rest Proposal	SC-28		
8	Proposed STIG and SRG Applicability Report	CM-2		
SD-02 Shop Drawings				
1	Network Communication Report	CA-9, CM-6, CM-7, PL-8, SC-8, SC-41		
2	Cybersecurity Riser Diagram	PL-2, PL-8		
SD-03 Product Data				
1	Control System Cybersecurity Documentation	SA-5		
SD-06 Test Reports				
1	Wireless Communication Test Report	AC-18		
2	Control System Cybersecurity Testing Procedures	RA-5		
3	Control System Cybersecurity Testing Report	RA-5		
SD-07 Certificates				
1	Software Licenses	CM-10		
SD-11 Closeout Submittals				
1	Confidential Password Report	IA-5		
2	Password Change Summary Report	IA-5		
3	Enclosure Keys	PE-3		
4	Software and Configuration Backups	CP-10		
5	Auditing Front End Software	AU-3		
6	Device Audit Record Upload Software	AU-3		
7	System Maintenance Tool Software	MA-3		
8	Control System Scanning Tools	MA-3		
9	STIG, SRG and Vendor Guide Compliance Result Report	CM-2		
10	Control System Inventory Report	CM-8, IA-3, SI-17		
11	Integrity Verification Software	MA-3		
TAA Compliance				
1	Vendor Trade Agreement Act Certificates	SA-12		



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.
2	Cybersecurity Riser Diagram	PL-2, PL-8	Approved	
SD-03 Product Data				
1	Control System Cybersecurity Documentation	SA-5	Approved	**Updated 7/26/22: Contractor provided submittal on 7/14/22.** Contractor stated “Will Submit Later” on submittal package dated 4/12/22.
SD-06 Test Reports				
1	Wireless Communication Test Report	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	Control System Cybersecurity Testing Procedures	RA-5	Not Applicable	Out of scope for UFGS 25 05 11 spec only. Contractor is directed to follow other specifications related to this topic.

NAVFAC FRCS CyCx Checklist Example: Red Zone After Action Report



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

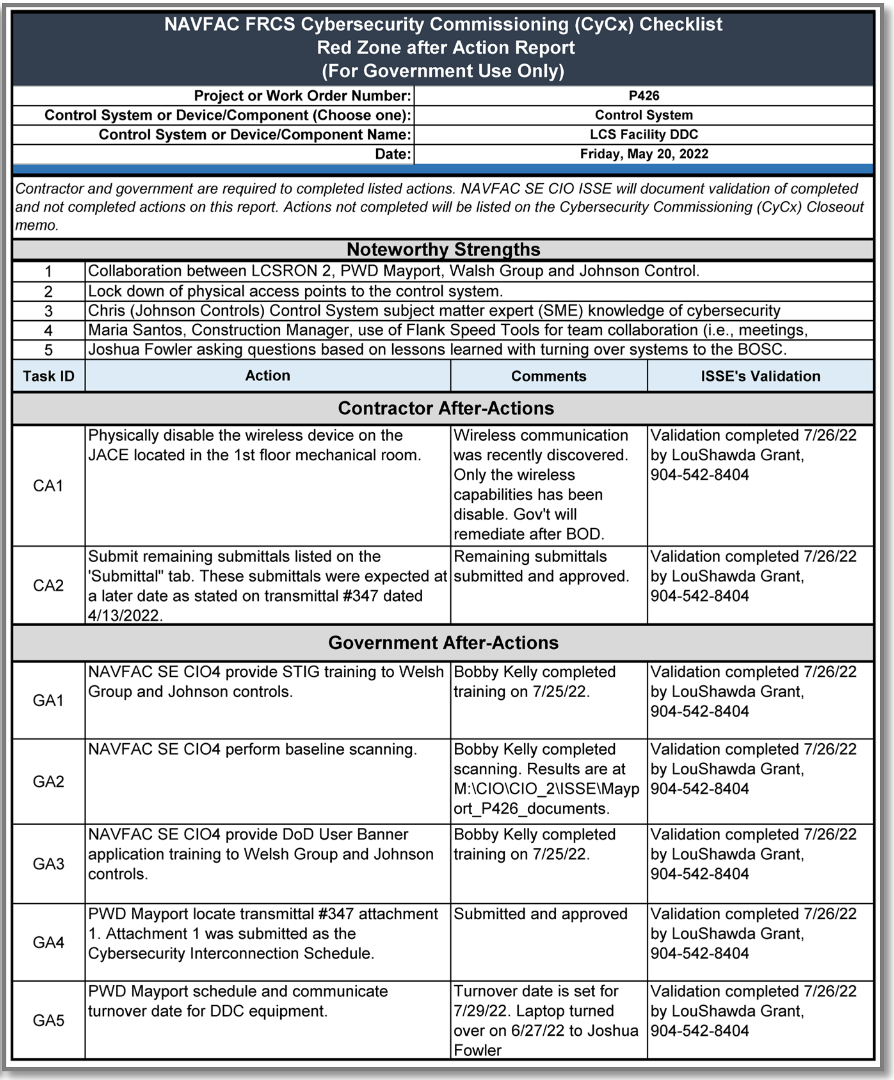
Project or Work Order Number:	
Control System or Device/Component (Choose one):	
Control System or Device/Component Name:	
Date:	

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 FRCS Cybersecurity Commissioning (CyCx) Closeout memo.

Noteworthy Strengths

1	
2	
3	
4	
5	

Task ID	Action	Comments	ISSE's Validation
Contractor After-Actions			
Government After-Actions			



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**

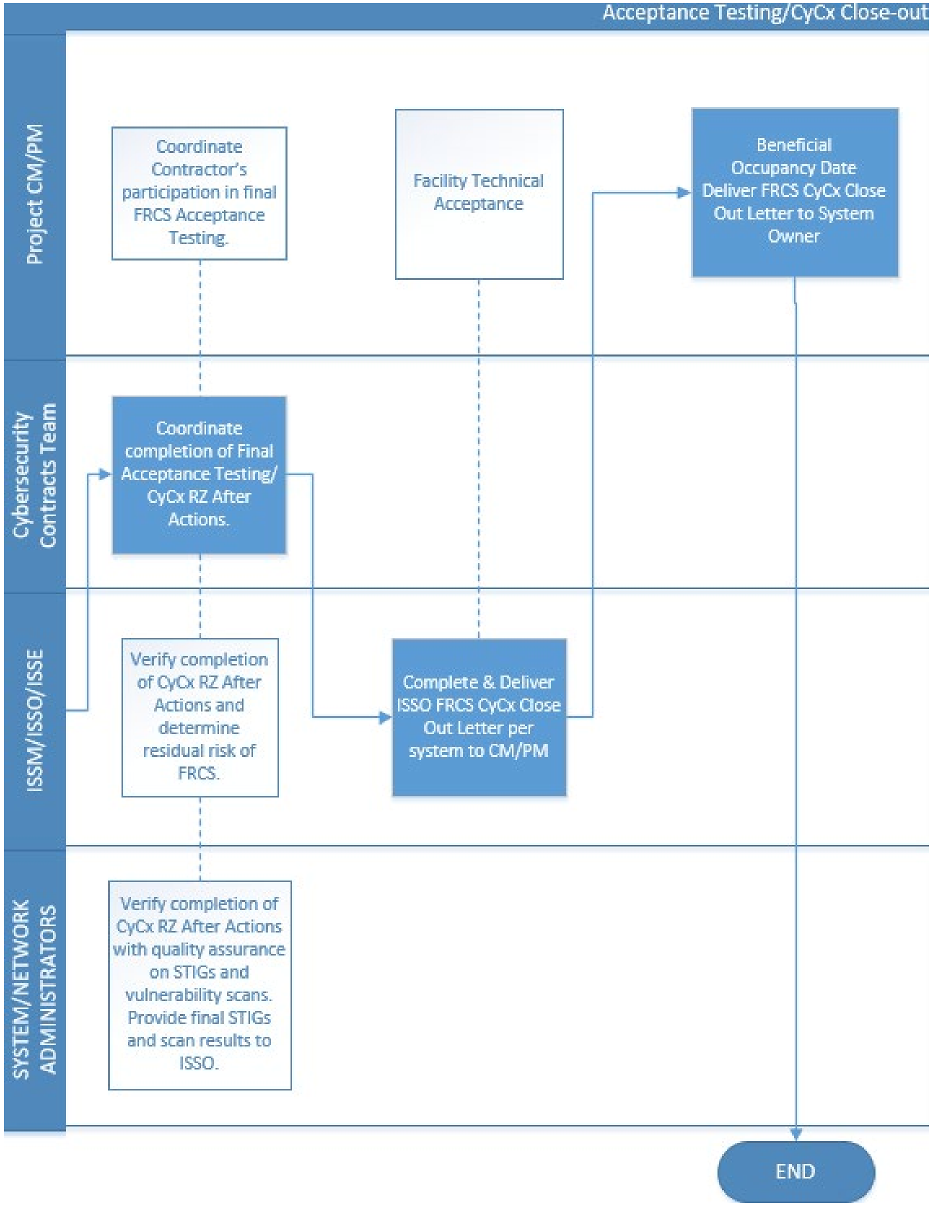
Contractor and government are required to completed listed actions. NAVFAC SE CIO ISSE will document validation of completed and not completed actions on this report. Actions not completed will be listed on the Cybersecurity Commissioning (CyCx) Closeout memo.

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

Close-Out Red Zone Commissioning Process



Acceptance Testing/CyCx Close-out

Project CM/PM

Coordinate Contractor's participation in final FRCS Acceptance Testing.

Facility Technical Acceptance

Beneficial Occupancy Date Deliver FRCS CyCx Close Out Letter to System Owner

Cybersecurity Contracts Team

Coordinate completion of Final Acceptance Testing/ CyCx RZ After Actions.

ISSM/ISSO/ISSE

Verify completion of CyCx RZ After Actions and determine residual risk of FRCS.

Complete & Deliver ISSO FRCS CyCx Close Out Letter per system to CM/PM

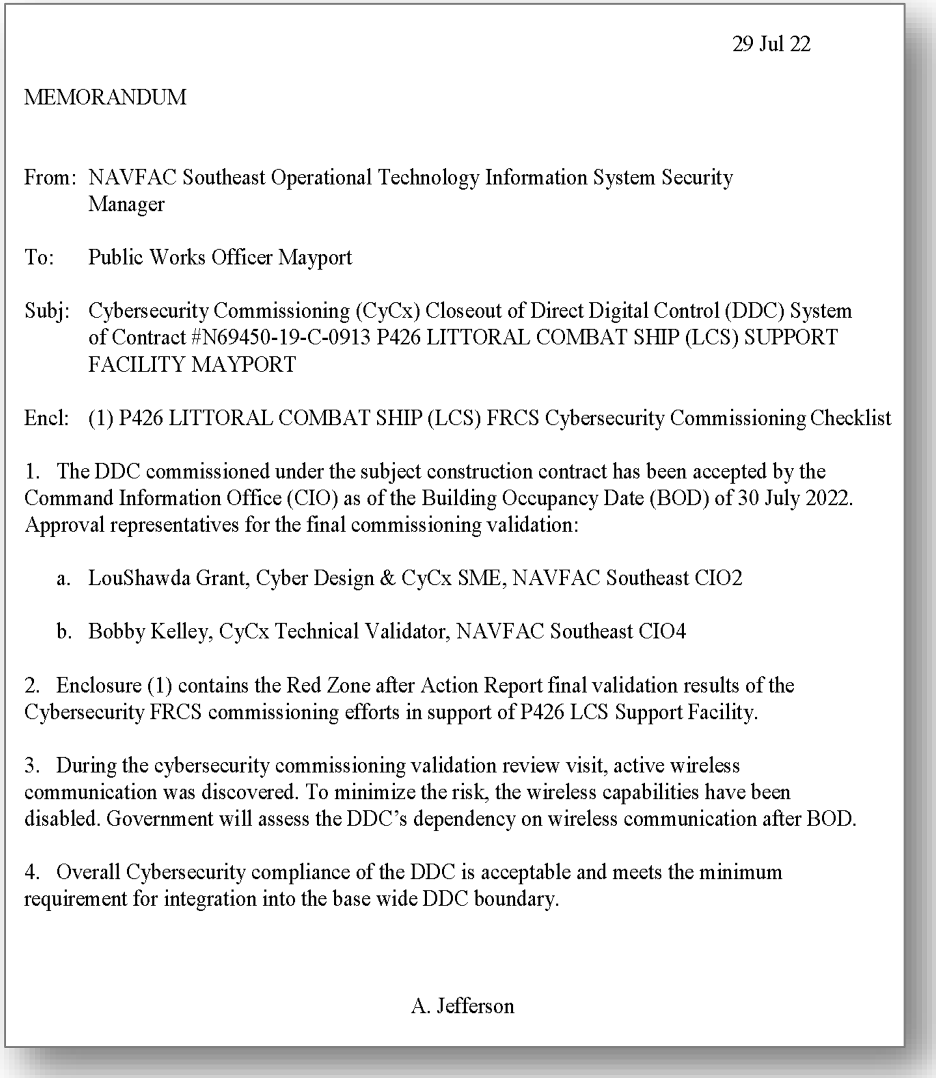
SYSTEM/NETWORK ADMINISTRATORS

Verify completion of CyCx RZ After Actions with quality assurance on STIGs and vulnerability scans. Provide final STIGs and scan results to ISSO.

END

CyCx Close-out Memorandum

- Provides a close-out letter to the System Owner
- 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)
- Provided to the Construction Manager for inclusion with Acceptance Testing Results



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

Red Zone CyCx Review

Red Zone Cybersecurity Commissioning (CyCx) is a method of evaluating whether the cybersecurity controls applied to a Facility Related Control System (FRCS) meet contract requirements using UFC and UFGS guides.

What Does Red Zone Cybersecurity Commissioning Accomplish?

- Helps determines what security controls are required by the contract and builds a *CyCx Checklist* specific to that contract
- Tracks Cybersecurity controls implementation through the use of the CyCx Checklist
- Provides an "After Action Report" after a Red Zone On-Site Assessment is performed
- Final Acceptance Testing is Performed in preparation for RZ close out
- **Close Out Memo** is provided to the System Owner at the end of the Red Zone Commissioning process outlining the overall cybersecurity contract compliance

Questions?