Cybersecurity Hygiene Checklist

Instructions: Please check the box in the completed field when you have executed the specified task. If you are unable to or do not complete a task, please provide an explanation and rationale in the comments box.

Task ID #	Tasks	Completed? Y/N	Responsible Party	Comments
Inventory				
1	An inventory of control system hardware and software was completed.			
2	The operational community shall perform inventory checks using the provided baseline, reporting results in an actionable fashion.			
3	Provide an accurate, complete, up-to-date, and timely inventory list, also known as a baseline list, of the approved hardware and software to the operational community. Store lists based on classification level.	Not in Contract (NIC)		
User / Password				
4	Wireless networks have passwords.			
5	Changed system default passwords, as appropriate.			
6	Educate the operator/technician on their responsibility for password/account protection	Not in Contract (NIC)		
7	Separated administrator and operator accounts, permissions, and passwords, as feasible.			
8	Passwords have been changed to meet DoD password standards, if feasible.			
9	When creating accounts or granting site access, follow the rule of least privilege, only granting access to the level necessary for completion of approved actions.			
10	Privileged accounts have been reviewed and restricted as necessary.			
11	Individuals with privileged access have signed privileged access form and background check has been completed.			
12	Reviewed and provided the appropriate user access rights, increasing or restricting access as needed based on access requirements.			
13	Unused accounts have been deleted.			
14	Identified whether shared credentials/accounts are utilized or not on this control system. Document result in comments.			
15	Ensure all recovery modes that can provide access to the system may only be accessed by unique accounts tied to individual users.			
16	Unless otherwise explicitly exempted, ensure the system limits access to recovery modes to individual users with a role requiring access.			
17	Role based permissions were implemented where feasible.			
Awareness				
18	Operators/technicians have been trained/educated on not installing new software unrelated to operations and maintenance of the system (e.g., games, chat, gambling,	Not in Contract (NIC)		

19	Validated that personnel interacting with control system have completed annual cybersecurity training. (IA awareness online).	Not in Contract (NIC)		
20	Educated the operator/technicians that changes to the control system may have a cybersecurity impact and require coordination with CIO.	Not in Contract (NIC)		
Process				
21	Update Regional cyber-incident response plan (IRP) for any unique requirements associated with this control system.	Not in Contract (NIC)		
22	System logs have been reviewed and appropriate actions taken based on log content.	Not in Contract (NIC)		
23	Create and document cyber-preventative maintenance focusing on, at a minimum, the following core tasks: scanning, patching, reporting, configuration management (CM), log file analysis, and HBSS/Host Intrusion Preventions System, (HIPS).			
Connectivity				
24	Modems or other devices used for remote (off-site) access were disabled/removed.			
25	Disconnect vendor remote access.			
Physical Access				
26	Documented who has control over access to control system equipment locations (electrical, mechanical, communications rooms).	Not in Contract (NIC)		
27	Documented how CIO access to equipment locations is obtained to include after hours access.	Not in Contract (NIC)		
28	If system is located in classified area, Joint Personnel Adjudication System (JPAS) SMO code and POC are documented.	Not in Contract (NIC)		
29	Physical security of control system components was confirmed in the inventory.			
30	Ensure physical security of CS components was confirmed in the inventory and that access to CS components is based on need to know.			
31	Restrict use of unauthorized devices, such as personal mobile devices, in secure spaces.	Not in Contract (NIC)		
Hardware and Software				
32	Non-essential software has been removed (i.e. games, personal software, etc.) from any control system computers in the facility.			

_____ _____

CIO 2, NAVFAC *Date*

_____ _____

CIO 4, NAVFAC *Date*