Defense Health Agency

PROCEDURAL INSTRUCTION

Number 8370.01
April 18, 2022

DAD-FO

SUBJECT: Standard Isolation Architecture for Cybersecurity of Facility-Related Control Systems

References: See Enclosure 1

1. PURPOSE. This Defense Health Agency-Procedural Instruction (DHA-PI) based on the authority of References (a) through (c) and in accordance with the guidance of References (d) through (av), establishes the Defense Health Agency's (DHA) procedures for cybersecurity of Facility-Related Control Systems (FRCS) within DHA-administrated facilities supporting the Military Health System.

2. APPLICABILITY. This DHA-PI applies to DHA, DHA Components (activities under the authority, direction, and control of DHA), and the Military Departments (MILDEPS); and all personnel to include assigned or attached active and reserve members, federal civilians, authorized contractors supporting DHA (when required by the terms of the applicable contract), members of the Commissioned Corps of the Public Health Service, and other personnel assigned temporary or permanent duties to DHA or DHA Components.

3. POLICY IMPLEMENTATION. It is DHA's instruction, pursuant to References (i) and (j) that the DHA will implement procedures for assessing and mitigating cyber risk within DHA-administrated facilities through awareness programs, management strategies, and technological solutions. This includes:

a. Providing standards for cybersecurity of building communications, electronic safety, and building control systems (BCS) in the planning, design, and construction of FRCS.

b. Defining procedures to establish Standard Isolation Architecture (IA) for DHA FRCS.

c. Implementing Reference (m).

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. PROPONENT AND WAIVERS. The proponent of this publication is the Deputy Assistant Director (DAD), Financial Operations (FO). When activities are unable to comply with this publication the activity may request a waiver by providing justification that includes a full analysis of the expected benefits and must include a formal review by the activity's senior legal officer. The activity director or senior leader will submit the waiver request through their supervisory chain to the DAD-FO to determine if the waiver may be granted by the Director, DHA or their designee.

7. RELEASABILITY. **Cleared for public release**. This DHA-PI is available on the Internet from the Health.mil site at: https://health.mil/Reference-Center/Policies and is also available to authorized users from the DHA SharePoint site at: https://info.health.mil/cos/admin/pubs/SitePages/Home.aspx

8. EFFECTIVE DATE. This DHA-PI:

a. Is effective upon signature.

b. Will expire 10 years from the date of signature if it has not been reissued or canceled before this date in accordance with Reference (c).

/S/
RONALD J. PLACE
LTG, MC, USA
Director

Enclosures
1. References
2. Responsibilities
3. Procedures

Glossary

TABLE OF CONTENTS

FIGURES

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," September 30, 2013, as amended
(b) DoD Directive 5136.13, "Defense Health Agency (DHA)," September 30, 2013
(c) DHA-Procedural Instruction 5025.01, "Publication System," August 24, 2018, as amended
(d) United States Code, Title 10, Section 1073c
(e) DoD Instruction 6015.17, "Military Health System (MHS) Portfolio Management," January 13, 2012, as amended
(f) ANSI/ISA-TR99.00.01-2007, "Security Technologies for Industrial Automation and Control Systems," 2007[1]
(g) ASHRAE Publications, ASHRAE 90.1-2019, "Energy Standard for Buildings Except Low-Rise Residential Buildings," as referenced in WBGCNSSI 1253, Security Categorization and Control Selection for National Security Systems 2014[2]
(h) BICSI Publications, ANSI/BICSI 007-2020, "Information Communication Technology Design and Implementation Practices for Intelligent Buildings and Premises," 2020[3]
(i) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended
(j) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended
(k) Unified Facilities Criteria, UFC 4-010-06, "Cybersecurity of Facility-Related Control Systems," September 19, 2016, as amended
(l) DoD Directive 8140.01, "Cyberspace Workforce Management," October 5, 2020
(m) DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended
(n) U.S. Cyber Command Technical Report, "Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DoD) Industrial Control Systems (ICS)," Revision 2, March 2018[4]
(o) Joint Test and Evaluation (JT&E) Program, "Handbook for Self-Assessing Security Vulnerabilities & Risks of Industrial Control Systems on DoD Installations," December 19, 2012[5]
(p) Department of Veterans Affairs, "Office of Information & Technology Design Guide," February 2011
(q) Department of Veterans Affairs, "Telecommunications and Special Telecommunications Systems Design Manual," February 2016
(r) Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 12, 2013

[1] This reference can be found at: https://www.isa.org/products/ansi-isa-tr99-00-01-2007-security-technologies-for
[2] This reference can be found at: https://www.ashrae.org/technical-resources/bookstore/standard-90-1
[3] This reference can be found at: https://www.bicsi.org/standards/available-standards-store/single-purchase/bicsi-007-iot-intelligent-building
[4] This reference can be found at: https://apps.dtic.mil/dtic/tr/fulltext/u2/1056116.pdf.
[5] This reference can be found at: https://www.wbdg.org/files/pdfs/ics_handbook.pdf

(s) Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017
(t) International Society of Automation, ANSI/ISA-62443-4-2-2018, "Security for Industrial Automation and Control Systems, Part 4-2: Technical Security Requirements for IACS Components"[6]
(u) National Institute of Standards and Technology, Special Publication 800-60 Volume I Revision 1, "Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008
(v) National Institute of Standards and Technology, Special Publication 800-37 Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018
(w) National Institute of Standards and Technology, Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security," current edition
(x) DHA Interim Procedures Memorandum 18-015, "Cybersecurity Program Management," September 28, 2020[7]
(y) National Institute of Standards and Technology, Special Publication 800-115, "Technical Guide to Information Security Testing and Assessment," September 2008
(z) National Institute of Standards and Technology, Special Publication 800-12 Revision 1, "An Introduction to Information Security," June 2017
(aa) National Institute of Standards and Technology, Special Publication 800-88 Revision 1, "Guidelines for Media Sanitization," December 2014
(ab) National Institute of Standards and Technology, Special Publication 800-160 Volume 1, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," November 2016, as amended
(ac) National Institute of Standards and Technology, Special Publication 800-41 Revision 1, "Guidelines on Firewalls and Firewall Policy," September 2009
(ad) National Institute of Standards and Technology, Special Publication 800-116 Revision 1, "Guidelines for the Use of PIV Credentials in Facility Access," June 2018
(ae) Unified Facilities Criteria, UFC 3-580-01, "Telecommunications Interior Infrastructure Planning and Design," June 1, 2016, as amended
(af) Unified Facilities Criteria, UFC 4-510-01, "Design: Military Medical Facilities," May 30, 2019, as amended
(ag) DoD Unified Facilities Guide Specifications, UFGS-25 10 10, "Utility Monitoring and Control System (UMCS) Front End and Integration," February 1, 2019
(ah) National Fire Protection Association, NFPA 101, "Life Safety Code," current edition
(ai) The Industrial Internet Consortium, "The Industrial Internet of Things Volume G1: Reference Architecture," Version 1.9, June 19, 2019
(aj) The Industrial Internet Consortium, "The Industrial Internet of Things Volume G4: Security Framework," September 26, 2016
(ak) DoD Directive 3020.40, "Mission Assurance (MA)," November 29, 2016, as amended
(al) DoD Instruction 3020.45, "Mission Assurance (MA) Construct," August 14, 2018

[6] This reference can be found at: https://www.isa.org/products/ansi-isa-62443-4-2-2018-security-for-industrial-au
[7] This reference can be found at: https://info.health.mil/cos/admin/pubs/DHA%20Publications%20Signed/Cybersecurity%20Program%20Management%20(Updated).pdf and can only be accessed with a government issued common access card (CAC)

(am) MIL-STD-882E, "Department of Defense Standard Practice, Safety System," May 11, 2012[8]
(an) Federal Energy Regulatory Commission, Order No. 706, "Mandatory Reliability Standards for Critical Infrastructure Protection," January 18, 2008
(ao) DHA "Plan 3: Implementation Plan for the Complete Transition of Military Medical Treatment Facilities to the Defense Health Agency," Version 6, August 12, 2019
(ap) DHA-Administrative Instruction 066, "Director's Critical Information Requirements (DCIRs) Situation Report (SITREP)," July 21, 2017, as amended[9]
(aq) Office of Management and Budget Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 3, 2017
(ar) DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, as amended
(as) DoD Manual 5400.11, Volume 2, "DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan," May 6, 2021
(at) DoD Manual 6025.18, "Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance In DoD Health Care Programs," March 13, 2019
(au) DoD Instruction 8580.02, "Security of Individually Identifiable Health Information in DoD Health Care Programs," August 12, 2015
(av) DoDI 4000.19, Support Agreements," December 1, 2020

[8] This reference can be found at: https://assist.dla.mil/online/doc_analysis/doc_info_general.cfm?ident_number=36027 and is available to registered users of the Defense Standardization Program ASSIST website
[9] Per DHA-AI 066, this DHA-AI is available to users with Common Access Card authorization on the DHA SharePoint site at: http://www.health.mil/dhapublications

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DHA. The Director, DHA will:

a. Maximize efforts to protect facilities from cyber threats by requiring facilities in design, construction, or operational status to adhere to a dynamic set of cybersecurity principles based on cybersecurity industry best practices per references in Enclosure 1 and through input offered by functional experts within the MILDEPS and industry partners.

b. Carry out DHA's responsibility to implement a Cybersecurity program based on the availability of funding within the program under which the control system (CS) was purchased and/or is maintained.

2. CHIEF, CYBERSECURITY DIVISION FOR DHA. The Chief, Cybersecurity Division must:

a. Implement procedures to process Authority to Operate (ATO) packages and assist in developing guidance, procedures, and requirements related to achieving DoD Cybersecurity goals and objectives.

b. Provide consulting services to DHA Facilities Enterprise (DHA-FE) and assist with certification requirements for the DHA Information Technology (IT)/FRCS workforce, as well as implementation and sustainment requirements, including the necessary supporting tools and resources.

c. Provide IT support for the necessary security features of the Isolation Architecture (IA).

d. Ensure that the Med-COI configuration and the IA will provide a defendable and monitored space protecting the DHA FRCS network from vulnerabilities with Defense-in-Depth configurations.

e. Draft, maintain, and administer security policies related to FRCS, including:

(1) Access Policy

(2) Connection Policy

(3) Change Management Policy. (NOTE: Local Change Management Policies must consider Mission Assurance categorization as documented on an approved Mission Assurance Asset List.)

(4) Threat Development Policy

(5) Overall, coordinated Incident Response Procedure Policy

f. Collaborate with DHA-FE and the DAD Infrastructure and Operations (IO) to ensure proper implementation of features unique to DHA FRCS that are atypical within traditional IT systems.

3. DAD-FO. The DAD-FO will:

a. Review and submit program and budget requirements for military construction (MILCON) and sustainment, restoration, and modernization pursuant to guidance of the ASD(HA) for the DoD Planning, Programming, Budgeting, and Execution process.

b. Provide programmatic oversight of the Defense Wide (Medical) MILCON and DHA Operations and Maintenance appropriations in accordance with instructions issued by the ASD(HA), fiscal guidance issued by the Under Secretary of Defense (Comptroller)/Chief Financial Officer, and applicable law.

4. CHIEF, DHA-FE. The Chief, DHA-FE must:

a. Support facilities capabilities at the Med-COI Network Operations Security Center.

b. Develop guidance, procedures, and requirements related to achieving DoD Cybersecurity goals and objectives with respect to facility-related CS.

c. Inform Cybersecurity Division of new facility projects. Incorporate DHA DAD-IO established processes for submission of ATO packages into the DHA-FE project life cycle.

d. Draft, maintain, and administer security policies related to DHA FRCS. Collaborate with DHA Cybersecurity Division and Infrastructure and Operations to ensure proper implementation of features unique to FRCS that are atypical within traditional IT systems.

e. Develop policies and procedures to enable:

(1) FRCS training

(2) Password Policy

(3) FRCS Incident Response Procedure Policy

(4) FRCS Inventory Management.

f. Develop, in collaboration with other Directorates as required, Risk Management Framework (RMF) packages and necessary artifacts to obtain an ATO.

g. Maintain an accurate and detailed inventory of FRCS, their interconnections, and the mission or function they serve.

5. DAD-IO. The DAD-IO will:

a. Appoint the Authorizing Official (AO) for ATO packages in accordance with Reference (i).

b. Advise DHA-FE and DHA Cybersecurity Division on IT engineering, architecture, and other related services in addition to providing traditional IT services, such as storage and cryptography.

c. Design, implement, manage, and operate the Level 3 Boundary Protection Demilitarized Zone (DMZ) and FRCS Levels 4 and 5.

d. Design, implement, manage, and operate the Test and Development Environment (TDE) used to validate patches, software updates, other approved changes, and revised Security Technical Implementation Guide configurations.

6. SECRETARIES OF THE MILDEPs. The Secretaries of the MILDEPs will:

a. Adhere to guidelines and processes in References (i) through (k), (u), and (w) to ensure medical facilities not migrated to the Med-COI are incorporated in the MILDEPs cybersecurity program for FRCS.

b. Reference the Office of the Deputy Assistant Secretary of Defense for Environment & Energy Resilience (E&ER) Platform IT Control System Master List for determining the preliminary impact values for the RMF "Step 1 – Categorize System" process.

7. DIRECTORS, DHA MARKET, SMALL MARKET AND STAND-ALONE MILITARY MEDICAL TREATMENT FACILITY ORGANIZATION (SSO), AND DEFENSE HEALTH AGENCY REGION (DHAR). The Directors, DHA Markets, SSO, and DHAR (known collectively throughout this publication as "DHA Components"), must coordinate with DHA-FE regarding Market-focused facilities requirements via the DHA Components-based Facilities Liaison as prescribed in Reference (ao) as follows:

a. Serve as a communication contact point for disseminating information between the DHA Components and DHA-FE.

b. Represent the DHA Component managers' cybersecurity responsibilities.

c. Provide DHA Component facilities status updates, forward Director's Critical Information Requirements, and coordinate Market-driven demand signals as cited in References (ao - ap).

d. Support DHA-FE led DHA Component-based facilities master planning efforts.

e. Defend information networks, secure data, and mitigate risks to the mission by adhering to the DHA guidelines when implementing facility cybersecurity measures for existing buildings.

8. DIRECTORS, DHA MTF, Dental Treatment Facility (DTF), and Veterinary Treatment Facility (VTF). DHA MTF, DTF, VTF Directors, must:

a. Defend information networks, secure data, and mitigate risks to the mission by adhering to the DHA guidelines when implementing facility cybersecurity measures for existing buildings.

b. Implement a program to ensure adherence to DHA Cybersecurity guidelines. Implement periodic inventories and audits to identify vulnerabilities and gaps in the DHA FRCS, as well as enforce the local change management procedures.

c. Advocate for funding to implement DHA Cybersecurity guidelines, close Cybersecurity gaps, and mitigate Cybersecurity vulnerabilities.

9. FACILITY MANAGERS, DHA. The Facility Managers, DHA must:

a. Coordinate, conduct, and maintain accurate inventories of all devices within the IA in accordance with applicable policies and standards for FRCS inventories. This may include hardware (physical devices and systems) and software (communications platforms and applications) Level 2 to Level 0 within the IA. Maintain accurate documentation of the network boundary, data flow diagrams and ports, protocols, and services used within the FRCS.

b. Follow the RMF process as outlined in References (i) through (k) and in DHA specific policy and guidance.

c. Be responsible for the system and data of FRCS.

d. Reference the E&ER Platform IT Control System Master List for determining the preliminary impact values for the RMF "Step 1 – Categorize System" process.

e. Collaborate with the Acquisitions community to accurately define security requirements and prioritize FRCS acquisitions with cybersecurity measures already incorporated into the design of the asset.

10. PROGRAM MANAGERS, DHA. The Program Managers, DHA must:

a. Be responsible for the DHA Facilities Installation Contractor submittals, Factory Acceptance Testing, Site Acceptance Testing, Penetration Test, and Commissioning reports provided by the agent.

b. Be responsible for these procedures and guidelines as the minimum standard Level of Cybersecurity Service for the DHA administered on-installation or leased assets.

c. Be responsible for the RMF processes as outlined in References (i) through (k) and in DHA specific policy and guidance.

d. Collaborate with the Acquisitions community to accurately define security requirements and prioritize FRCS acquisitions with Cybersecurity measures already incorporated into the design of the asset.

e. Advocate for funding to implement DHA Cybersecurity guidelines, close Cybersecurity gaps, and mitigate Cybersecurity vulnerabilities.

ENCLOSURE 3

PROCEDURES

1. BASIS FOR PROCEDURES

a. Procedures in this document are based on the RMF process outlined in References (i) through (k), and additional RMF guidance posted on the RMF Knowledge Service webpage: https://rmfks.osd.mil/rmf/Pages/default.aspx.

b. Procedures standardization within DHA helps to achieve costs savings, improve overall quality installation, and maximize returns on information technology and facility investments. It also reduces costs and improves cybersecurity for DHA FRCS by focusing on planning, programming standards and criteria, and outfitting facilities to provide the most strategic cybersecurity defense in depth for the DHA.

c. Procedures are based on best practices within cybersecurity such as safety, security, and resilience in addition to utilizing a common set of policies for people, processes, strategy, and technology for protecting FRCS.

d. Procedures include training and education guidance for facilities staff, specifically the knowledge and tools needed to effectively manage and protect mission critical and/or life safety systems within the DHA.

2. FRCS BACKGROUND

a. FRCS are integrated hardware and software designed to monitor and control the operation of equipment, infrastructure, or associated devices. FRCS consist of a combination of technology such as computers/servers and Human-Machine Interfaces plus control components such as electrical switches, mechanical actuators, and sensors that act together upon underlying equipment to achieve a physical objective. Various categories of FRCS include:

(1) Supervisory Control and Data Acquisition (SCADA) Systems. Highly distributed systems used to monitor and control geographically dispersed assets where centralized data acquisition, control, and status reporting are critical to system operation.

(2) Distributed Control Systems (DCS). Used to control specific processes within a facility. DCS are integrated control architectures that provide supervisory-level control and integration over subsystems responsible for local process control.

(3) Programmable Logic Controller (PLC). Proprietary processor-based, solid-state devices found in almost all control equipment and processes to provide logic algorithms for connected input and output devices. They can vary in sophistication from simple, stand-alone microcontrollers to sophisticated, multi-processor controllers that provide advanced motion

control, network capability, error detection, diagnostics, process recovery, and fail-safe redundancy. While a PLC is a component of DCS and SCADA systems, it is often the solitary control device for smaller FRCS configurations used to provide operational control of separate processes.

b. Historically, FRCS were neither automated nor networked and, in general, fundamentally lacked desired IT features such as cryptographic capabilities, logging, and password protection. Devices used for monitoring or control had no computing resources and those that were digitized typically used proprietary protocols and PLCs rather than full computer control. As controllers became interconnected, they were not designed with traditional IT system and security considerations, as they were expected to operate as isolated systems running on their own dedicated network with proprietary communication protocols and specialized hardware and software. This intentional separation from traditional IT (e.g., email, web access, networked printing, or remote access) allowed FRCS to be easily connected, open and accessible, highly stable, deterministic, and readily serviced. Today, however, FRCS are designed using standard platforms, operating systems, network protocols, and access controls commonly found in traditional IT systems. The ever-increasing connectedness of FRCS allows for greater operational capabilities, efficiencies, and automation. However, this integration also introduces new vulnerabilities that expose both the FRCS and the underlying network to threats.

c. Special precautions must be taken when introducing IT security controls and solutions to FRCS environments because of the unique ways that FRCS communicate and operate. Interconnections between FRCS and organizational networks/business systems are a particular point of focus for security and should be carefully considered. In all cases, security solutions must be tailored to the specific FRCS environment and verified to ensure their impact to the FRCS is not detrimental to the operation of FRCS.

d. FRCS can have long life spans (often exceeding 20 years) and can be comprised of technology that suffers rapid obsolescence. This longevity introduces several issues. Most importantly, older hardware and software may no longer be supported by the manufacturer. Companies can go out of business or terminate their support for an installed product. Because of this, patches and forward support for compatibility with new operating systems may no longer be available as new vulnerabilities are discovered.

e. In the traditional IT domain, where data is the preeminent priority, cybersecurity often focuses on preventing the disclosure of information to unauthorized individuals or processes. Consequently, confidentiality tends to be the most important attribute among the three properties of the confidentiality-integrity-availability triad. However, with FRCS, it is paramount to actively manage or monitor physical processes and maintain high availability and positive control of the system. Therefore, availability and integrity of the FRCS take precedent over confidentiality. It is this difference in cybersecurity priorities that impacts what security controls and procedures are appropriate to implement for FRCS compared with those of traditional IT.

f. Networked FRCS are those systems which have multiple controllers and can have both traditional Internet Protocol (IP) traffic at Level 3 and up, and traditional IP along with other ethernet and serial traffic at the lower levels. Depending on the age and type of CS, these CS

may have the capability for remote monitoring, and/or existing vendor service level agreements may recommend remote access. A Business-to-Business agreement is required for remote access and monitoring. There are two types of networked FRCS:

(1) Internally Networked, also designated as Stand-alone Information Systems, which have multiple components networked together but does not have a network connection to anything that is not part of the CS; and

(2) Externally Networked, where the CS has multiple components networked together and does connect to a network that is not part of the CS.

g. Non-networked FRCS are generally those that consist of a single controller and do not have the capability for remote monitoring.

3. SYSTEMS CATEGORIZATION AND DEFINITIONS

a. Control Systems are defined by the E&ER Enterprise Mission Assurance Support Service (eMASS) Control Systems Master List. Systems not listed are not exempt from categorization.

b. System designers and system owners will develop a list of systems requirements that will support the functional operations of the facility.

c. Data will be classified in accordance with Reference (u).

d. Most common FRCS information types include:

(1) C.2.8.12 General Information

(2) C.3.1.1 Facilities, Fleet, and Equipment Management Information Type

(3) C.3.4.2 Inventory Control Information Type

(4) C.3.5.8 System and Network Monitoring Information Type

(5) D.4.4 Emergency Response Information Type

(6) D.7.1 Energy Supply Information Type

(7) D.7.2 Energy Conservation and Preparedness Information Type

(8) D.7.4 Energy Production Information Type

(9) D.13.1 Training and Employment Information Type

(10) D.13.3 Worker Safety Information Type

(11) D.16.5 Property Protection Information Type

(12) D.20.2 General Purpose Data and Statistics Information Type

(13) D.20.4 Knowledge Dissemination

(14) D.22.3 Public Resources, Facility, and Infrastructure Management

e. The Standard Isolation Architecture provides a zone for each system type including but not limited to:

(1) Zone: Med-Industrial Control System. Zone contains systems and subnets that control the function of the facility and do not access, use and/or manipulate data/information categorized as Personally Identifiable Information (PII), Payments Information, or Protected Health Information (PHI) and where adverse cyber operation of the system does not immediately endanger human well-being.

(a) Subnet Med-Utility Monitoring and Control Systems (UMCS). Contains the following systems:

1. Cathodic Protection Systems

2. Direct Digital Control for Heating Ventilation and Air Conditioning (HVAC) (Mission Essential)

3. Direct Digital Control for HVAC (Mission Support)

4. Electrical Systems

5. Generator Monitoring and Alarm System

6. Lighting Control Devices

7. Natural Gas System

8. Potable Water System

9. Pure Water Systems

10. Sanitary Sewer/Wastewater System

11. Shade Control System

12. Facility Underground Fuel-Oil, Storage Tanks

13. Uninterruptible Power Supply System

14. UMCS

15. Vehicle Charging System

16. Weather Monitoring System

(b) Subnet Med-Vertical Transportation System. Contains Elevators (Controls) systems.

(c) Subnet Med-Stand-alone Information System. Contains the following systems:

1. Airfield Control

2. Automatic Guided Vehicle Systems

3. Cable Television Premises Distribution System

4. Cart Wash System

5. Clock System (Network Time Synchronization)

6. Electronic Message Signage (Wayfinding)

7. Fume Hood Alarm System

8. Infrared and Radio Frequency Tracking Systems

9. Integrated Audio-Video Systems and Equipment

10. Internal Cellular and Antenna Systems

11. Pneumatic Tube System

12. Radio and Public Address Systems

13. Refrigerator Monitoring Systems

(d) Subnet Med-Medical Gas. Contains Gas and Vacuum Systems for Healthcare Facilities systems.

(2) Zone: Med-LIFE. Zone contains systems and subnets that control the function of critical facility systems that are life safety in nature or use, access and/or manipulate data/ information categorized as Life Safety and where adverse cyber operation of the system will endanger human well-being. These systems do not access, use, or manipulate data/information categorized as PII, Payments Information, or PHI. The Fire Detection and Alarm System is contained in the Subnet MED-FAS.

(3) Zone: Med-Electronic Security System (ESS). Zone contains systems and subnets that control the function of facility ESSs. These systems may require access to and manipulate data/information categorized as PII and/or PHI and where adverse cyber operation of the system may endanger human wellbeing. The ESS is contained in the Subnet Med-ESS.

(4) Zone: Med-MED. Zone contains systems and subnets that control the clinical and clinical support systems of a facility not to include Personal Property Medical Devices (except where integrated into a system). These systems may require access to and manipulate data/information categorized as PII, and/or PHI and where adverse cyber operation of the system may endanger human wellbeing. Escalated handling or separate security control overlay requirements for these systems will be evaluated by the system owner and Authorizing Official. The Subnet Med-MED contains the following system: Nurse Call System.

(5) Zone: Med-PWR. Zone contains systems and subnets that control facility power generation systems. These systems may use, access and/or manipulate data/information categorized as Life Safety and where adverse cyber operation of the system may endanger human well-being. These systems do not access, use, or manipulate data/information categorized as PII, Payments Information, or PHI. The Subnet Med-PWR contains the following systems:

(a) Microgrid

(b) Utility Metering System (Advanced Meters, Advanced Metering Infrastructure, etc.)

(6) Zone: Med-QUAR. Zone contains existing legacy systems that cannot meet modern security standards and may be completely isolated from connectivity with other systems. These systems will not use, access, and/or manipulate data/information categorized as PII, Payments Information, or PHI.

4. RMF. All MILCON will adhere to References (k), (w), and (x), and DoD RMF guidance outlined in References (j) and (m) to the greatest extent possible to sufficiently manage the life cycle cybersecurity risk of FRCS.

5. RISK CATEGORIZATION

a. Reference (k), in conjunction with References (am) and (an), will determine overall risk categorization.

b. Preliminary Confidentiality-Integrity-Availability triad determination of systems will be per E&ER eMASS Control Systems Master List, and the DHA-FE Program Management Office Baseline Categorization Memo for Facility Related Control Systems. The final system categorization will be coordinated with the System Owner and AO.

c. Variations are permitted with approval of AO.

6. STANDARD ISOLATION ARCHITECTURE

a. Standard Reference Model. Designers and system owners will implement the features of Reference (k) Figure E-1 "5-Level Control System Architecture" and Reference (t) to the greatest extent possible.

b. Usage of Med-COI Infrastructure. Services of the Med-COI will be leveraged to greatest extent possible in support of Mission Assurance and will include:

(1) Department of Defense Information Network (DoDIN) protection procedures, features and practices required per Reference (m), and (n).

(2) Help desk and support

(3) Network time synchronization

(4) Domain Name Server service

(5) All communication with external networks

(6) System-to-system communication across zone boundaries of varied risk categorizations

(7) Patch and change management of Med-COI assets

c. Segregated Responsibilities and Ownership

(1) A Memorandum of Agreement will be developed, in accordance with Reference (av), for each installation that clearly and completely defines the separation of responsibilities between IT and Facility organizations.

(2) To the greatest extent possible, physical and operational ownership of the Personal and Real Property architecture components may be segregated between traditional IT and traditional facility functions.

(a) Owned and operated by Med-COI – "Traditional IT"

(b) Owned and operated by Facilities – "FRCS Isolation Architecture"

(3) A Boundary Protected DMZ will be implemented at Level 3 to facilitate data transfer between Med-COI and FRCS Isolation Architecture(s). Devices and services can be built by Med-COI as necessary and may include:

(a) Med-COI side firewall

(b) FRCS side firewall

(c) Usage of uni-directional gateway devices. Uni-directional gateways may not be used as drop-in replacements for firewalls.

(d) Asynchronous reporting historian

(e) Anti-Virus/Malware deployment server

(f) Security Information and Event Management aggregator

(g) Patch deployment server

(h) Jump host

(4) Access to Internet, enterprise email systems, and all other business services is prohibited in the FRCS network or beyond the Level 3 Boundary Protection DMZ.

(5) Direct trust relationship(s) between FRCS and other business networks is prohibited. System owners are encouraged to provide reasonable means to access business networks, on separate machines from FRCS, to allow for adherence to this requirement.

(6) The following figure graphically represents the logical interface of Med-COI and Facilities for the Standard Isolation Architecture.

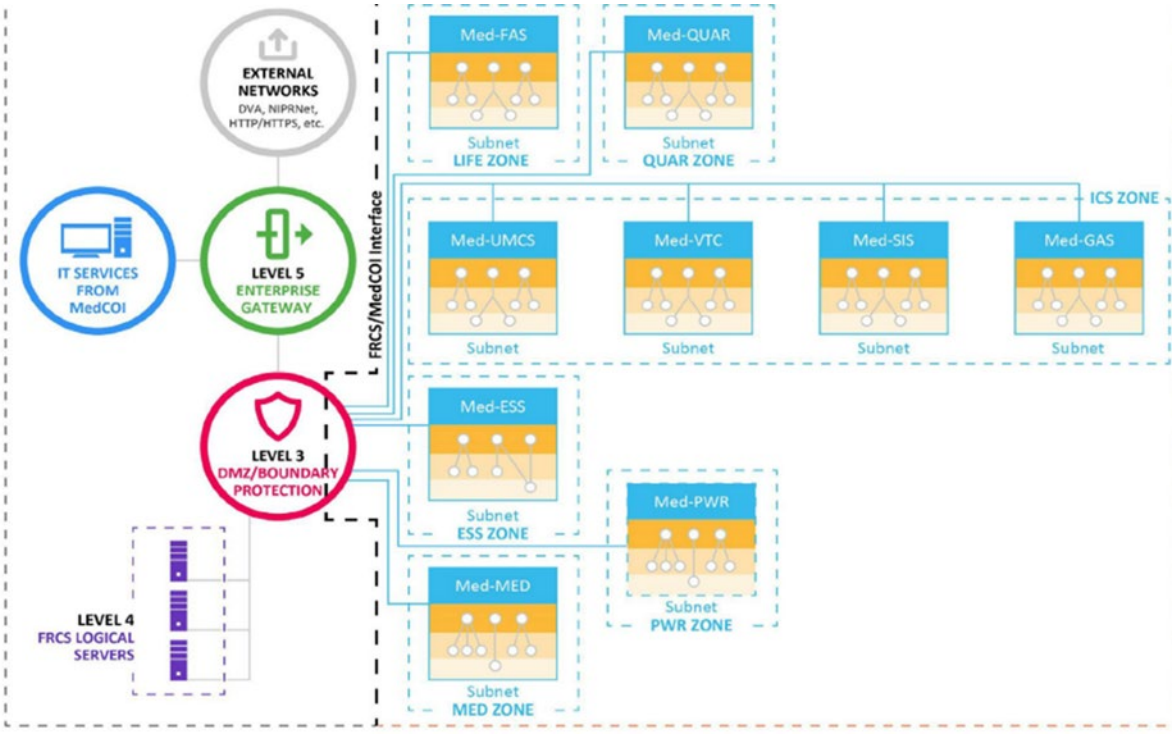

Figure 1. Segregation of Medical Community of Interest and Facility-Related Control Systems Isolation Architecture

(a) Adherence to References (j) and (m), maintenance and operation of the following will be the responsibility of Med-COI:

1. Level 3: Boundary Protection and DMZ. This includes activities outlined in the Joint Information Environment Cybersecurity Reference Architecture as required for a Special Purpose Processing Node.

2. Level 4: FRCS Logical Processors, including servers and workstations.

3. Level 5: Enterprise Gateway, including all components.

(b) Adherence to References (j) and (m) directs that maintenance and operation of Level 0, 1, and 2 devices and components for FRCS will be the responsibility of Facilities.

(c) Facilities will own, maintain, and operate all cabling and devices up to the Level Boundary Protection DMZ.

(7) Communications between systems that are life safety in nature or mandated by code will be wholly owned and operated by facilities.

d. System, Subnet and Zone Assembly

(1) The following figures graphically represent the assembly of demonstrative systems, subnets, and zones.

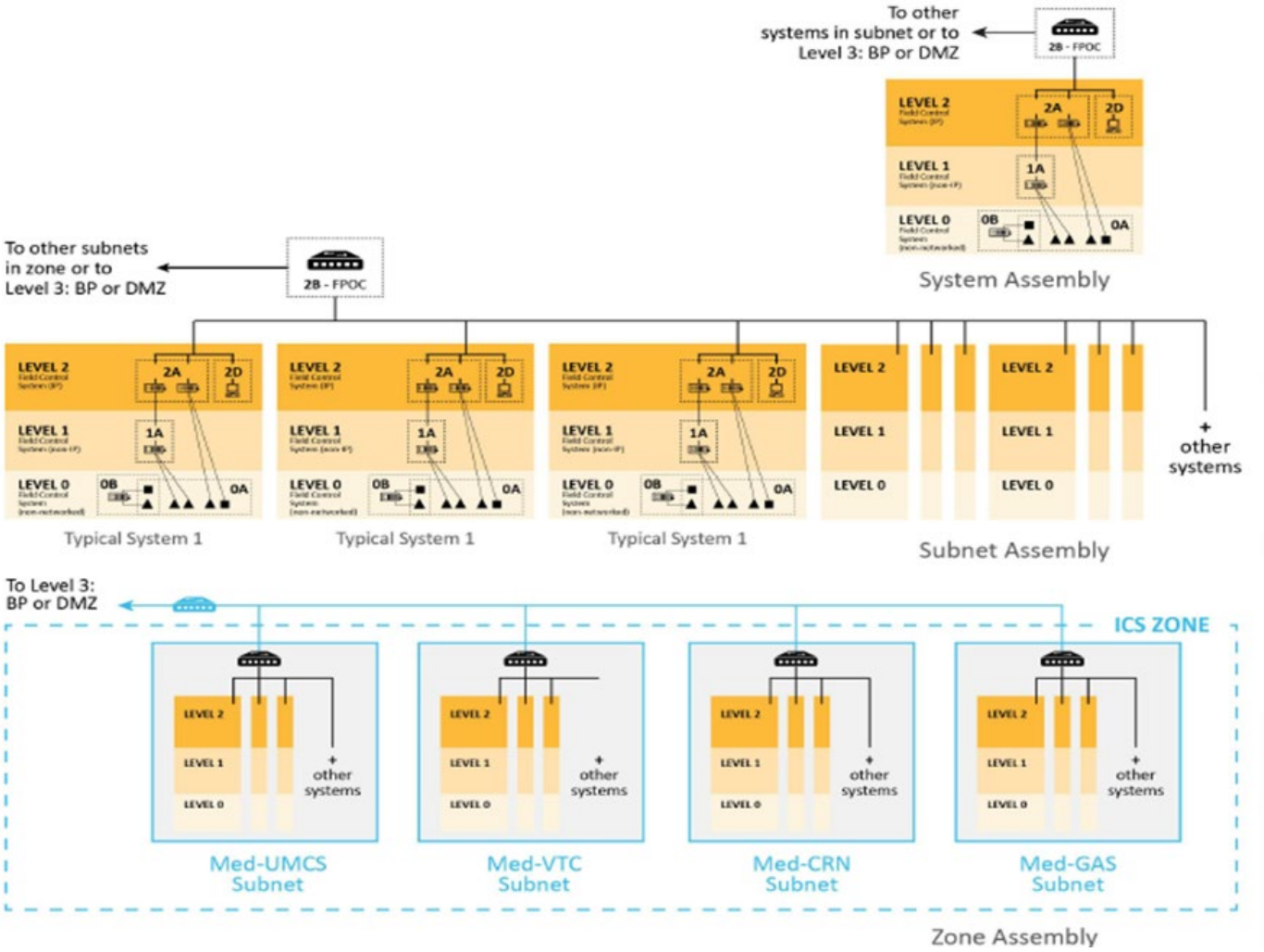

Figure 2. System, Subnet, and Zone Assembly Representation

(2) FRCS will be designed and installed to operate in a code-driven, minimal or reduced functionality state, independently using components of Level 0, 1, and 2.

(3) FRCS may interface, without crossing Level 3 Boundary Protection DMZ, within zone.

(4) Systems should interface at a common Level 2B Field Point of Connection (FPOC).

(5) FRCS interface with Med-COI infrastructure will occur at the Level 3 Boundary Protection DMZ.

(6) A group of one or more systems of same categorization and similar risk, connected by layer two network infrastructure comprise a subnet.

(7) FRCS domain controller may be provided at Level 2 with the intent to maintain survivability in the event of an outage.

(8) Inbound and outbound zone communication will pass through Level 3 Boundary Protection DMZ at the facilities side firewall. Circumventing this logical communication flow is prohibited.

(9) Zones may be separated to allow for group policy, patch, and change management customization at the zone level.

e. Adapted 5-Level Architecture

(1) Appendix E of Reference (k) governs elements not modified by the following requirements:

(a) Derived from Figure 2-1 in Reference (k).

(b) Simplification of Level 3 to allow for improved ownership severability.

(c) Additional FPOC's at Level 2 to allow for multi-zone implementations.

(d) Added representative DMZ architecture for Med-COI and FRCS network data exchange.

(2) The following is a simplified representation of the Adapted 5-Level architecture for a multi-zone, multi-subnet, multi-system installation leveraging Med-COI for infrastructure.

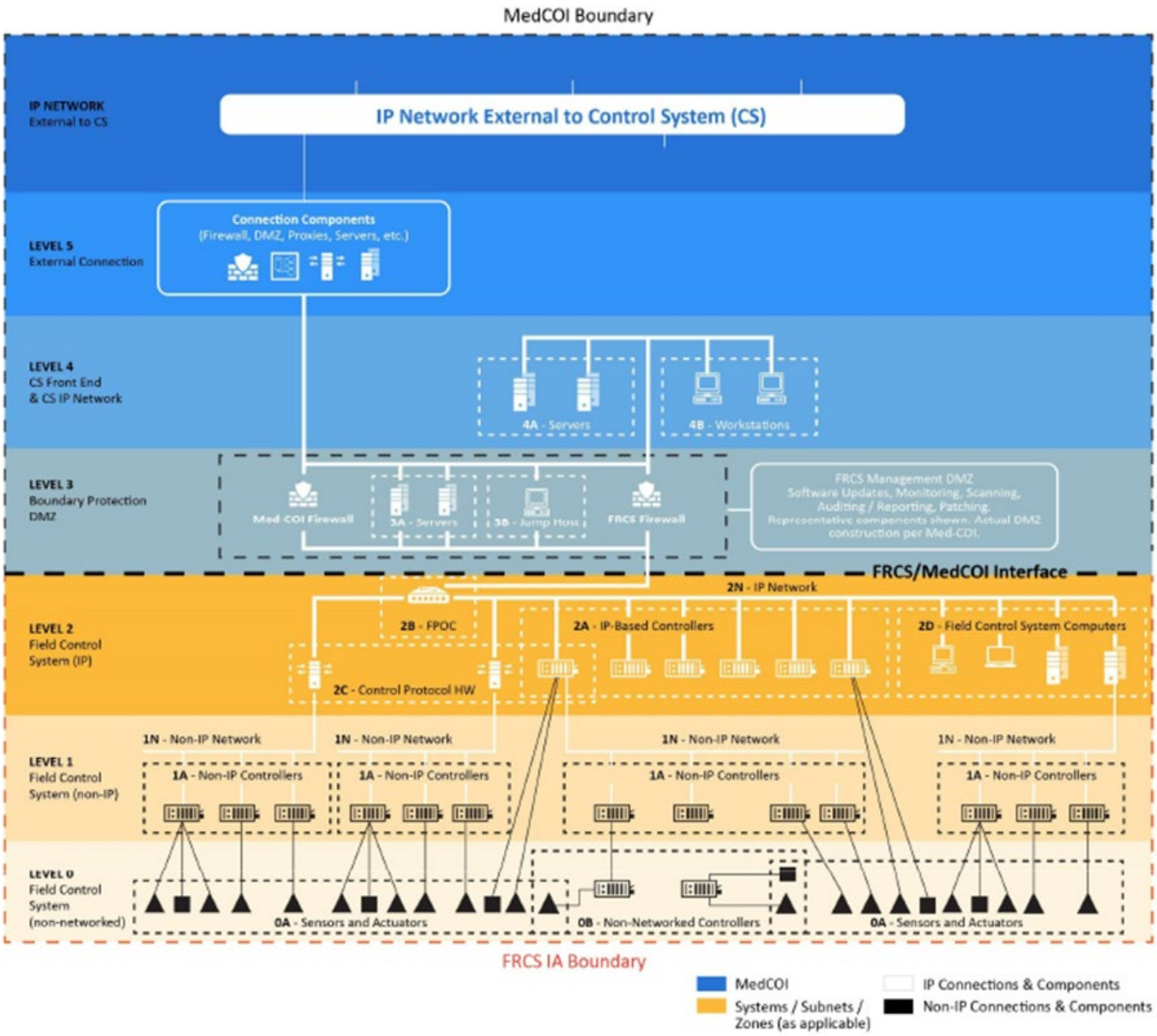

Figure 3. Adapted 5-Level Architecture

f. System to System Communication

(1) Reference (k), Chapter 4 will be utilized.

(2) Minimize FRCS operational reliance on Med-COI services so that when operating in an isolated mode, FRCS functionally is not unacceptably diminished.

(3) Direct communication between systems and subnets within a single zone permitted without restriction.

(4) For Level 0, 1, and 2 direct communication to external networks, as defined as any network that is not directly responsible for the supervision, monitoring or control of the FRCS, is prohibited.

(5) Zone to zone communication requires logical validation by the Level 3 Boundary Protection and/or Level 4 Logical Servers for acceptability in addition to typical screening procedures.

(a) Typical Screening. In accordance with Reference (m).

(b) Logical Screening. Level 4, Logical FRCS servers/workstations, will actively screen data calls and commands of lower-level systems that seek responses from systems in other zones by white listing, leveraging the following logical communication flow. DHA subject matter experts will develop specific whitelisting procedures on a project-by-project basis.

1. Logs of request handling will be maintained as required by Reference (m).

2. System controller in a zone makes the data call/command directly, and only, to the Level 4, FRCS Logical Server.

3. Level 4, FRCS Logical Server, deconstructs the packet and reviews the request against programmed white list procedures with one of the following results: 1 - Requests on white list are processed accordingly or 2 - Requests not on white list are passively denied and alarm displayed.

4. Level 4, FRCS Logical Server, the packet is reassembled, if required, into the receiving system communication port and protocol then issued directly to that system.

5. The receiving system processes the request with one of the following results: 1- Single direction request is processed. Communication complete or 2- Feedback requests are routed directly back to the Level 4, FRCS Logical Server to be handled the same as an initial request.

7. STANDARD ISOLATION ARCHITECTURE ADAPTATIONS

a. For facilities projects, variations to the architecture are permitted with approval coordinated through DHA-FE.

b. As authorized by the AO, installations may provide an independent DoDIN in substitution of leveraging Med-COI infrastructure. Requirements of Reference (m) for standalone DoDIN must be met. Circuits must be procured via the DHA Circuit Management Office as part of the DHA portfolio.

8. TDE

a. The Systems Integrator will build or augment and maintain a TDE within the DAD IO TDE that replicates the Production Environment to the highest degree possible starting with the Level 4 Workstations, Servers, FRCS software and with at least one of each of the Level 3-0 major components, devices, and actuators. The TDE will be used to perform Factory Acceptance Testing of the FRCS to ensure the system has end-to-end functionality; has been properly configured using the Security Content Automation Protocol (SCAP) tool and the Security Technical Implementation Guides; and has had all applicable patches installed and properly configured.

b. The TDE will be used to conduct Site Acceptance Testing of the completed FRCS, and if required, penetration testing.

9. PREPARING FOR AND RESPONDING TO A BREACH OF PII

a. References (aq) - (au) describe Federal and DoD policy on privacy and the requirement to prepare for and respond to a breach of Personally Identifiable Information (including Protected Health Information).

b. If a breach occurs or is suspected, the discovering party will report such a breach to the DHA Privacy Office within 24 hours, at (703)-275-6363. The information should also be forwarded via email to the DHA Privacy Officer at dha.privacyofficer@mail.mil. If such breach is a cybersecurity incident, the discovering party will report this event to the U. S. Cyber Command within 48 hours of the potential cybersecurity incident.

10. GUIDANCE FOR LEASED FACILITIES. Contact DHA-FE at: dha.ncr.facility-plan.mbx.frcspmo@mail.mil for leased facility guidance.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AO	Authorizing Official
ATO	Authority to Operate
BCS	Building Control System
CCTV	closed-circuit television system
CS	Control System
DCS	Distributed Control System
DHA	Defense Health Agency
DMZ	Demilitarized Zone
DoDIN	Department of Defense Information Network
DTF	Dental Treatment Facility
E&ER	Environment and Energy Resilience
eMASS	Enterprise Mission Assurance Support Service
ESS	Electronic Security System
FCS	Field Control System
FE	Facilities Enterprise
FPOC	Field Point of Connection
FRCS	Facility-Related Control Systems
HVAC	Heating Ventilation and Air Conditioning
IA	Isolation Architecture
IDS	Intrusion Detection System
IP	Internet Protocol
IT	Information Technology
Med-COI	Medical Community of Interest
MILDEPs	Military Departments
MILCON	Military Construction
MTF	Medical Treatment Facility
PHI	Protected Health Information
PII	Personally Identifiable Information
PLC	Programmable Logic Controller
RMF	Risk Management Framework

SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
TDE	Test and Development Environment
UCS	Utility Control System
UMCS	Utility Monitoring and Control System
VTF	Veterinary Treatment Facility

PART II. DEFINITIONS

AO (NIST SP 800-37 Rev 2). A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.

Building Automation System. The system consisting of a UMCS Front End, connected BCS which control building electrical and mechanical systems, and user interfaces for building control supervision. The Building Automation System is a subsystem of the UMCS. This term is being phased out in favor of UMCS.

BCS. A building control system is a system that controls building electrical and mechanical systems such as HVAC (including central plants), lighting, vertical transport systems, and irrigation systems. BCS generally do not have a full-featured user interface; they may have "local display panels" but typically rely on the UMCS front end for full user interface functionality. BCS is a subsystem of the UMCS and is a class of Field Control System.

closed-circuit television system (CCTV). An ESS that allows video assessment of alarm conditions via remote monitoring and recording of video events. Video monitoring may also be incorporated into other systems which are not CCTV.

CS. A system of digital controllers, communication architecture, and user interfaces that monitor, or monitor and control, infrastructure and equipment.

Controller. An electronic device – usually having internal programming logic and digital and analog input/output capability – which performs control functions. Two primary types of controllers are equipment controller and supervisory controller.

DCS. This term is being phased out in preference of BCS, Utility Control System (UCS), and/or UMCS.

DHA Sustained Facility. A facility sustained by the Defense Health Agency (DHA) that is either managed by DHA or managed via a DHA facility contract in accordance with Section 1073c of

Title 10 United States Code, as indicated by a "DHA" sustainment organization code in the DoD Real Property Inventory. Military Department (MILDEP) medical readiness facilities are also considered a "DHA Sustained Facility" if there is a Memorandum of Agreement (MOA) in place that transfers Facility Sustainment, Restoration, Modernization (FSRM) funds for those facilities to DHA.

ESS. The integrated electronic system that encompasses interior and exterior (physical) intrusion detection systems (IDS), CCTV systems for assessment of alarm conditions, access control systems, data transmission media, and alarm reporting systems for monitoring, control, and display.

Energy Monitoring Control System. Another name for a UMCS. See definition for UMCS.

Equipment Controller. A controller implementing control logic to control a piece of equipment. NOTE: a controller is defined by use, and many equipment controllers also have the capability to act as supervisory controllers. Some examples of equipment controllers are air handler controllers, protective relays, and pump controllers. Note that some devices, such as power meters or smart sensors, which only perform monitoring functions, are still considered equipment controllers (despite not actually controlling anything).

FRCS. A controls system which controls equipment and infrastructure that is part of a DoD building, structure, or linear structure. FRCS, a subset of Platform Information Technology is defined as including but not limited to: buildings and their associated control systems (building automation systems or building management systems, energy management systems, fire and life safety, elevators, etc.); utility distribution systems (such as electric, water, waste water, natural gas and steam); telecommunications systems designed specifically for industrial control systems including supervisory control and data acquisition; direct digital controls, programmable logic controllers, other control devices and advanced metering and sub-metering devices. DoD FRCSs are clearly delineated from other types of industrial control systems by being physically located on DoD property.

Field Control System (FCS). A BCS, UCS, Access Control System, etc. within the Facility and "downstream" of the FPOC.

Field Control Network. The network used by the BCS, UCS, etc., within a facility "downstream" of the FPOC. This includes IP, Ethernet, RS-485, Free Topology Twisted Pair TP/FT-10 and other network infrastructure that support control system(s) in a given facility.

FPOC. The FPOC is the point of connection between the ICS IP network and the Field Control Network (an IP network, a non-IP network, or both). The hardware which provides the connection at this location is an IT device such as a switch, IP router, or firewall.

Impact. The effect on organizational operations, organizational assets, or individuals due to a loss of Confidentiality, Integrity, or Availability in the CS. Impact is categorized as one of three levels:

a. LOW: limited adverse effect

b. MODERATE: serious adverse effect

c. HIGH: severe or catastrophic adverse effect

NOTE: The impact level of a system is generally written in ALL CAPS for clarity.

Incident. An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies

ICS. One type of control system. Most specifically a control system, which controls an industrial (manufacturing) process. Sometimes also used to refer to other types of control systems, particularly utility control systems such as electrical, gas, or water distribution systems.

IT. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

IDS [Physical/ESS]. A system consisting of interior and exterior sensors, surveillance devices, and associated communication subsystems that collectively detect an intrusion of a specified site, facility, or perimeter and annunciate an alarm.

IDS [Cyber]. A device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to management.

IA. The physical protection, and systematic encapsulation of information exchanges internal to a system component. This is done through the hierarchical organization of information exchanges until the inadequate legacy systems with obscure proprietary communication are secured.

Life Safety. Data and/or a cyber physical activity that endeavors to protect human well-being.

Protected Health Information (PHI). Individually identifiable health information that is transmitted or maintained by electronic or any other form or medium. PHI excludes individually identifiable health information in employment records held by a DoD covered entity in its role as employer. Information which has been de-identified in accordance with Paragraph 4.5.a is not PHI. PHI is a subset of PII, with respect to living persons.

PII. Personally identifiable information' means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Platform IT. IT, both hardware and software, which is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

Reference Architecture. A standard based open architecture. It provides guidance for the development of system, solution, and application architectures, providing a common vocabulary and definitions in the system of interest, with which to discuss the implementations.

Risk. A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Risk Management. The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

SCAP. A method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., Federal Information Security Management Act compliance). The National Vulnerability Database is the U.S. Government content repository for SCAP.

SCADA. This term is being phased out in preference of BCS, UCS, and/or UMCS.

Supervisory Controller. A controller that implements a combination of supervisory logic (global control or optimization strategies), scheduling, alarming, event management, trending, web services, or network management. A supervisory controller may be located between the Platform Enclave and the FCS serving as the data aggregation conduit between the FCS and the front end. Note that this arrangement is defined by use; many supervisory controllers have the capability to also directly control equipment and serve the role of both supervisory controller and equipment controller.

UCS. A type of FCS used for control of utility systems such as electrical distribution and generation, sanitary sewer collection and treatment, water generation and pumping, etc. Building controls are excluded from a UCS, however it is possible to have a UCS and a BCS in the same facility, and for those systems to share components such as the FPOC. A UCS is a subsystem of a UMCS and is a class of FCS.

UMCS. The system consisting of one or more BCS and/or utility control systems and the associated UMCS Infrastructure. In other words, it is the complete utility monitoring system – from the front end to equipment controllers. At the highest level the UMCS is composed of a

UMCS Platform Enclave and UMCS Front End (jointly referred to as UMCS Infrastructure) and connected FCS(s).

Vulnerability. Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.