DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Building Technologies Technical Reference Guide

Version 3.0

May 1, 2024

Approvals

DocuSigned by:
Phil Klokis
6F8E4C8418E2469...

Phil Klokis
Associate Chief Information Officer
GSA Information Technology: Office of Public Buildings Information Technology Services

DocuSigned by:
Bo Berlas

Bo Berlas
Chief Information Security Officer
GSA Information Technology: Office of the Chief Information Security Officer

DocuSigned by:
Courtney Springer

Courtney Springer
Assistant Commissioner
Public Buildings Service: Office of Facilities Management

DocuSigned by:
Charles G Hardy

Charles Hardy
Chief Architect
Public Buildings Service: Office of Architecture and Engineering

DocuSigned by:
Robert Carter

Robert Carter
Associate Administrator
Office of Mission Assurance

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Table of Contents

Approvals **1**
Table of Contents **2**
Introduction **6**
Chapter 1: Policy, Standards and IT Security Requirements **9**
1.0 Overview 9
1.1 BMC Systems Roles and Responsibilities 9
1.2 Policies and Requirements for Interconnectivity 10
1.2.1 Trusted Internet Connection (TIC) 10
1.2.2 Cellular Connection 11
1.2.3 Government Furnished Equipment 11
1.2.4 BMC Systems Device Whitelisting Process 12
1.3 GSA Network Access to Perform Duties 12
1.3.1 HSPD-12 Credentialing and Systems Privileges 12
1.3.2 Background Investigations 12
1.4 BMC Systems Device, Appliance and Software Security Assessment Process 13
1.4.1 GSA IT Security Scanning Process 13
1.4.1.1 Step 1: Pre-Assessment 13
1.4.1.2 Step 2: Induction 17
1.4.1.3 Step 3: Assessment 18
1.4.1.4 Step 4: Initial SAR Issuance 18
1.4.1.5 Step 5: Vendor Remediation/Final SAR Issuance 18
1.4.1.6 Step 6: BMC Systems Service and Support 18
1.4.2 Wireless Assessments 19
1.4.3 Encryption 21
1.4.4 Non-Standard Software Review Process (BSN Console Software) 21
1.4.5 Variable Refrigerant Flow (VRF) in HVAC Controls 22
1.5 Building Systems Network (BSN) 22
1.5.1 BSN Operations and Maintenance Roles and Responsibilities 23
1.5.2 BSN Evolvement and Implementation 23
1.5.2.1 History of BSN 23
1.5.2.2 Current Implementation of BSN (Trustsec and Microsegmentation) 24
1.5.3 Standard BSN Configurations 25
1.5.4 Steps to Integrate Sites onto the BSN 26
1.6 Incident Response (IR) and Building Recovery (BR) Exercises 27
1.6.1 Incident Response 27
1.6.2 Building Recovery Exercises 27
Chapter 2: Network Infrastructure **29**
2.0 Overview 29
2.1 Network Roles and Responsibilities 29

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

2.2 Standards for Interoperability 30
2.3 Network Topology 31
2.3.1 Network Design Requirements 31
2.3.2 Sample Network Design Diagram 33
2.4 Requesting and Installing a GSA Circuit 33
2.4.1 How to Locate the Demarc Room and Demarc Extension Room 34
2.4.2 How to Request a GSA Circuit and the Installation Process 34
2.4.3 Important Considerations in the Circuit Installation Process 36
2.5 Hardware Standards and Policy 36
2.5.1 Requesting and Installing Switches 36
2.5.2 Installing and Connecting Hardware 36
2.5.2.1 Types of Connections Allowed 37
2.5.2.2 Alternate Connectivity Options For Approved BMC Devices 37
2.6 BACnet 38
2.6.1 How Does BACnet Make Use of IP Networks? 39
2.6.2 BACnet Key Definitions 39
2.6.3 Implementing BACnet on a Wide Area Network (WAN) 40
2.6.3.1 UDP Port Assignment 41
2.6.3.2 BACnet/Ethernet 41
2.6.3.3 Using a BACnet Broadcast Management Device (BBMD) 42
2.6.3.4 Foreign Device Registration 42
2.6.3.5 BACnet/IP Multicast 42
Chapter 3: Cabling 43
3.0 Overview 43
3.1 Cabling Roles and Responsibilities 43
3.2 Cabling Infrastructure Standards 43
3.2.1 Minimum Requirement for Ethernet Cabling 44
3.2.2 Attenuation Limit 44
3.2.3 How are GSA IT Cabling Standards Enforced? 45
3.3 Cabling Installation 45
Chapter 4: BMC Systems Servers 46
4.0 Overview 46
4.1 BMC Systems Server Roles and Responsibilities 46
4.2 BMC Server Standards 46
4.2.1 Why Go Virtual? 46
4.2.2 BMC Systems Server Hardware and Software Specifications 47
4.2.3 BMC Systems Application Requirements 48
4.3 BMC Systems Deployment Process 48
4.3.1 Step 1: Submit BMC Server Request Form 49
4.3.2 Step 2: Schedule Server Solutions Meeting with TechOps 49
4.3.3 Step 3: Server Deployment Process 49
4.3.4 Do’s and Don'ts for Application Installations 50
4.4 Application Access 50
4.4.1 How to Request Different Types of Access 51

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

4.4.2 Methods for Accessing an Application via Web Browser 52
4.4.2.1 How to Request Access to a Web Application 52
4.4.2.2 How to Access a Web Application via Citrix VDI 52
4.4.2.3 How to Access a Web Application via BSN Console 53
4.4.3 Methods for Accessing an Application via RDP to a Server 54
4.4.3.1 How to RDP to a Server via Citrix VDI 54
4.4.3.2 How to RDP to a Server via BSN Consoles 57
4.4.3.3 How to Log Off a Remote Desktop Session on a BMC Systems Server 57
4.5 Server Maintenance and Support 58
4.5.1 Server Monitoring and Backup 58
4.5.2 Server Patching 59
4.5.2.1 Communications for BMC Systems Contacts 59
4.5.2.2 Planned Maintenance and Outages 60
4.5.2.3 Unplanned Maintenance and Outages 60
Chapter 5: BSN Consoles 61
5.0 Overview 61
5.1 BSN Consoles System Standards 61
5.2 How to Obtain a BSN Console 61
5.3 How to Access BSN Consoles 61
5.4 Installing Software on the BSN Console 62
5.5 BSN Console Maintenance and Support 62
Chapter 6: Technical Support for BMC Systems 63
6.0 Overview 63
6.1 Technical Support Roles and Responsibilities 63
6.2 Initial Troubleshooting Steps 64
6.3 Reporting a BMC Systems Issue 65
6.4 BMC Systems Support Workflow 67
6.4.1 BMC Systems Application Issue 67
6.4.2 BMC Systems Hardware 68
6.4.3 Network Issue 68
6.4.4 BMC Server Issue 68
6.4.5 BSN Console Issue 69
Chapter 7: Advanced Metering System (AMS) 70
7.0 Overview 70
7.1 Advanced Metering System Roles and Responsibilities 70
7.2 Advanced Metering System Architecture 71
7.3 Standards for Interoperability 72
7.4 New Installations 72
7.4.1 Sample Network Diagram 72
7.4.2 Cabling 73
7.5 Technical Support for AMS 73
7.5.1 Support Form 73
7.5.2 Troubleshooting Process 75
Chapter 8: Physical Access Control System (PACS) 76

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

8.0 Overview 76
8.1 Physical Access Control Systems Roles and Responsibilities 76
8.2 Security 78
8.3 PACS Architecture and Integration 78
8.4 Project Flow 79
8.5 GSA IT EPACS Support 81
Chapter 9: BMC Systems Procurement: Contract Language & IT Requirements in Scope of Work 82
9.0 Overview 82
9.1 Contract Language IT Security Requirements 82
9.2 Scope of Work Template (BAS Hardware/Software Upgrades) 88
Chapter 10: Best Practices for BMC Systems Project Implementations 97
10.0 Overview 97
10.1 Tips for Running a Successful BMC Systems Project 97
10.2 BMC Systems Checklist for Projects 100
10.2.1 Unitary Controller Configuration 100
10.2.2 Server/AMS Configuration 100
10.2.3 General Documentation and Deliverables 100
10.2.4 Application Account Administration 101
Appendix A: Contact Information 102
Appendix B: Listing of Reference Policies 102
Appendix C: Change Log 105

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Introduction

The nation's buildings are increasingly relying on Building Monitoring and Control (BMC) systems with embedded communications technology, and many are enabled via the Internet. While the advent of the Internet of Things (IoT) allows for ease of use, remote access, and data reporting/integration, it can also create easy targets for hackers and those with malicious intent. Attackers can exploit these systems to gain unauthorized access to facilities. These technologies can also be used as an entry point to the traditional informational technology (IT) systems and data which can cause physical destruction of building equipment and expose an organization to significant financial obligations to contain and eradicate malware or recover from a cyber-event. Federal facilities can include courthouses, laboratories, and regional office buildings, many of which are part of the nation's critical infrastructure. These facilities contain building control systems (i.e. heating, ventilation and air conditioning) as well as physical access control systems (i.e. electronic card readers and closed-circuit camera systems) that are increasingly being automated and integrated to other information systems or networks and the Internet. As these systems are becoming more integrated, so is their vulnerability to potential cyber-attacks.

As the world has learned from highly visible cybersecurity incidents at many large business organizations and the Office of Personnel Management (OPM), hacking is a growing trend. The external threats are real enough to raise concerns and the GSA does not want to be the next target. Cyber incidents can compromise Personally Identifiable Information (PII) and cause outages related to power, network, or other issues. This will cause major damage to the security infrastructure of a building, and it can also have a long-term rippling effect that can go on for many years. Building a platform with emphasis on security and disaster recovery in mind will limit these types of incidents as well as protect the infrastructure, including the building systems, which can be vulnerable to internal or external sources.

The Building Technology Services Division (BTSD) was established under GSA IT as a response to growing cybersecurity concerns related to Building Monitoring Control (BMC) systems. BTSD resides within the Office of GSA IT's PBS Public Building IT Services (PB-ITS) and specializes in IT Project Management support for building systems projects that depend on the GSA network or require remote connectivity. This includes new capital projects, system migrations and system upgrade projects. Additionally, BTSD creates standards, procedures, and provides guidance and resources for buildings located across the eleven PBS regions. BTSD is at the forefront of assessing and managing risk posed by hardware and software components of BMC Systems and works closely with IT Security to facilitate the BMC systems security assessment process. BTSD also supports network integration activities related to IoT technologies. BTSD serves in a cross-functional role, collaborating across multiple groups and organizations including:

- Office of Chief Information Officer (OCIO)/GSA IT
- Office of Facilities Management (OFM)
    - Smart Buildings Program
    - Energy Program Division
    - GSA Proving Ground (GPG)
- Office of Federal High Performance Buildings

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- Office of Mission Assurance (OMA)
- Office of Project Delivery

The Building Technologies Technical Reference Guide (BTTRG) was developed due to a growing demand for formalized guidance related to the technical integration of BMC Systems to the GSA network and within GSA's information technology (IT) environment. BMC Systems include, but are not limited to, building technologies such as building automation systems (BAS), advanced metering systems (AMS), lighting control systems (LCS), physical access control systems (PACS), renewable energy systems, and national digital signage (NDS). These systems, while closely related to the scope of facilities management, are IT systems and do collect GSA building data, and as such are subject to the same federal (i.e. the Federal Information Security Management Act (FISMA)) and agency specific policies and security standards as any other federal IT system. It is the intent of this document to inform on those policies and standards. Additionally, this document establishes a consistent and repeatable approach for how these technologies will be implemented and supported within GSA. The audience for this guide is facility managers, operations and maintenance staff, and potential and/or contracted vendors and integrators.

This guide was initiated and published by the Public Buildings Information Technology Services (PB-ITS) in participation with GSA IT Security, Office of Mission Assurance (OMA), multiple offices of PBS including Office of Facilities Management (OFM), Office of Design and Construction (ODC), as well as with participants from the regions. Each chapter of this guide covers a functional area and the content for each was developed through working group meetings, which included the participation of stakeholders and subject matter experts.

The BTTRG aligns with existing Federal and GSA specific IT policies and is partnered with the Technology Policy for PBS-Owned Buildings Monitoring and Control Systems (latest version posted on InSite). For guidance on smart building implementations and industry best practices for building automation systems, please refer to:

- GSA Smart Buildings Program Guide
- GSA Smart Building Implementation Guide
- GSA Data Normalization for Building Monitoring & Control Systems

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Revision History

Version	Date
Version 1.0	June 2011
Version 1.1	February 2014
Version 2.0	September 2016
Version 2.0	June 2021
Version 3.0	May 2024

This guide will be updated every few years to illustrate improvements to processes, evolved best practices, and any new or updated policies and standards relevant to the implementation of BMC Systems. Users of this guide are encouraged to provide feedback that will lead to improvements in future versions by emailing the BTSD at [redacted]

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Chapter 1

Policy, Standards, and IT Security Requirements

1.0 Overview

This chapter details the General Services Administration's (GSA) and Public Building Services' (PBS) standards and Information Technology (IT) security policies with respect to the implementation of BMC systems devices/applications. It documents the comprehensive system requirements related to approved software, standard hardware, network connectivity, user access, security clearances and Building Systems Network (BSN). Additionally, policies and procedures contained herein will guide PBS in preparing for assessment and authorization activities required for building systems projects.

Current policies for assessment and authorization of systems and devices on the BSN are based on the *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations* and the *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-213A, IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog*. The BSN servers supporting the BMC systems and associated devices have been issued a FISMA Moderate Authority to Operate (ATO). Additionally, the GSA IT Security Team has issued guidance and procedure documents. The documents cover the BMC systems security assessment process, roles and responsibilities and the Service Level Agreements (SLA) for evaluation.

1.1 BMC Systems Roles and Responsibilities

- **GSA IT Buildings Technology Services Division (BTSD):** The BTSD is the liaison between the Regional PBS Project Teams, vendors/contractors and GSA IT for all BMC systems that need to be integrated onto the GSA network. ***Please Note: See Section 1.5.4 for the steps on how to integrate a site onto the GSA network.***

- **GSA IT Network Operations and Management Team (Network Team):** The network team has command responsibility for the GSA Wide Area Network (WAN) and Local Area Network (LAN). They are responsible for the entire IP transport layer and are the sole provider for IP/subnet allocation at the building level. In addition, they manage network devices (i.e. routers and switches) and the BSN's connectivity. ***Please Note: PBS is responsible for the controllers/devices. GSA IT provides connectivity up to the switch port.***

- **GSA IT Technical Operations Team (TechOps):** TechOps is responsible for all PBS servers on the GSA network. This includes VMware/virtual server builds, operating systems (OS), databases, server/application services and system backups/restores. ***Please Note: See Chapter 4 for more details on TechOps's role in provisioning BMC systems servers.***

- **GSA IT Security Team:** The GSA IT Security Team is responsible for providing cybersecurity to PBS including endpoint protection, perimeter defense, vulnerability scanning and enterprise logging. They

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

perform regular scans of BSN servers as part of compliance validation. In addition, they are also responsible for authoring the Assessment and Accreditation (A&A) documents, performing risk assessments, managing system compliance over the life of the ATO and managing the POA&M items specific to the BSN.

- **GSA IT BMC Systems Security Assessment Team:** The BMC Systems Security Assessment Team performs hardware, firmware, and software assessments on devices designated as BMC systems components. They are also responsible for reporting the proper configuration of the device and any residual risks associated with use of the device within the GSA network. ***Please Note: See Section 1.4 for more details on the BMC Systems Security Assessment Process.***

- **Regional PBS Project Teams:** This includes regional Smart Building Team members, BAS specialists, contracting officers, project managers and facility management. They are responsible for ensuring that any BMC systems contracted, purchased, owned and/or operated in the regions adhere to all GSA policy and implementation guidance. They are also responsible for the installation, configuration, and management of the application hardware, firmware and/or software. In addition, the regions are responsible for contacting the BTSD prior to the award for applicable contract and implementation requirements. ***Please Note: See Chapter 4 for links to required documents.***

- **Vendor/Contractor:** The vendor/contractor is responsible for adhering to GSA IT policies. This includes ensuring BMC systems hardware, firmware and software meet Security Assessment Report (SAR) provisions and provide maintenance/support of their products connected to the GSA network.

1.2 Policies and Requirements for Interconnectivity

The following section provides information regarding GSA IT policies and standards with which PBS-IT systems, vendors, manufacturers, and integrators shall comply.

1.2.1 Trusted Internet Connection (TIC)

Trusted Internet Connections (TIC) is a mandate from the Office of Management and Budget (OMB). The purpose is to reduce the number of internet gateways on the federal government network and to ensure that all external connections are routed through a government agency that has been designated as an approved TIC Access Provider. All BSN network traffic must transit through a TIC, which is a network circuit that is managed by GSA IT.

2100.1P CIO GSA Information Technology (IT) Security Policy (latest version as of May 2024) states:

“All GSA owned or managed network devices must maintain a connection to a GSA facility, which handles GSA data shall be strategically positioned behind a GSA firewall to provide analysis/correlation, management structure, and minimize threats presented by external attacks.”

TIC will allow GSA to provide monitoring, incident response, vulnerability assessment/management, incident reporting, engineering support, and the enforcement of the agency’s specific security policy at the hosted facility. It will also allow trained, qualified, and cleared staff to support security functions 24x7.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

external/commercial network connection for managing or monitoring of building systems in any GSA owned, non-delegated, building will not be tolerated. Such connections will be removed upon discovery.

1.2.2 Cellular Connection

BMC systems devices are to be connected to the GSA Building Systems Network. GSA realizes that under certain circumstances, connecting BMC systems devices to the Building Systems Network is not feasible, and other network transport technologies may need to be employed. The use of a cellular transport is by exception only, based on a GSA OCISO risk assessment. All cellular transport must be facilitated by a device with the following security capabilities: stateful firewall, audit logging, and VPN. GSA IT security must be provided administrative access to the device facilitating the cellular transport. All BMC systems devices utilizing cellular transport must successfully complete the BMC Systems Security Assessment Process and undergo annual penetration tests. The GSA OCISO may grant exceptions to the security capabilities based on the results of a GSA OCISO risk assessment. ***Please Note: All cellular connections, whether they are a part of the GSA network or not, are subject to security testing and validation.***

1.2.3 Government Furnished Equipment

Federal Acquisition Regulation (FAR) Part 45 defines Government Furnished Equipment (GFE) as "equipment that is owned by the government and delivered to, or made available to a contractor". As such, GFE hardware must be used to access IT systems. This applies to all networking infrastructure, IP enabled devices, servers and workstations associated with BMC systems. Citrix VDI can be used as an alternative to GFE, when applicable. Vendor-provided computer hardware is not allowed to connect to the GSA network and can only be used for pre-commissioning purposes. If vendor-provided devices, workstations, or servers are discovered, they are subject to removal without warning.

- **Network Equipment:** This includes, but is not limited to, any equipment that provides networking capabilities, i.e. routers, switches, and wireless access points (WAP). ***Please Note: WAPs are provisioned on a case-by-case basis. The use of WAPs to support BMC systems is under review. Please discuss with your BTSD IT PM for the latest information.***

- **Computer Hardware**: This includes servers, printers, computers, smart devices, and their peripherals (monitors, mice, and keyboards), etc.

As buildings are integrated with the GSA network, GSA IT will make every effort to provide at least one laptop to these sites. The purpose of the laptop is to provide building management staff with access to their BMC systems application interfaces. Facility managers and project managers are responsible for ensuring that the GFE are in a locked IT closet or secure location that only approved/cleared personnel can access.

Please Note: Availability of hardware is dependent on the availability of funding. Existing GSA workstation refreshes will still be coordinated through the regional GSA IT manager's office. Hardware (switches, laptops, etc.) will not be provided unless an approved network diagram is submitted. See Section 2.4 for details about network diagram requirements and submission.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

1.2.4 BMC Systems Device Whitelisting Process

Cisco Identity Services Engine (ISE) is an identity and access-control policy platform that allows enforcement of security and access policies for endpoint devices connected to GSA's routers and switches. ISE is a mandated security policy to ensure that unauthorized systems are not connected to the network. It is applied to GSA switches which, in turn, block devices that are not recognized as approved devices, including rogue circuits and unmanaged switches.

The GSA rolled out the Mac Address Bypass (MAB) process in June 2017. For a device to be allowed to communicate over the GSA network, its MAC address must be whitelisted by GSA IT. All devices will need to be remediated before they are whitelisted. ***Please Note: See Section 1.4 for details on the BMC Systems Security Assessment Process.***

1.3 GSA Network Access to Perform Duties

This section demonstrates how any GSA employee, contract staff, or vendor personnel can obtain access to GSA IT systems, which includes all hardware, system software, data, and network access. Each of these requirements must be met for access to be granted. ENT domain credential and VPN access require a *Homeland Security Presidential Directive-12 (HSPD-12): Policy for a Common Identification Standard for Federal Employees and Contractors* adjudication. ***Please Note: To ensure uninterrupted support from vendor personnel, government sponsors/project POCs must ensure vendor personnel maintain their ENT accounts and keep them active. This includes timely completion of all tasks required to keep an ENT account active, such as annual IT Security Training courses, and regularly logging into their email.***

1.3.1 HSPD-12 Credentialing and Systems Privileges

Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (HSPD-12) is a mandated policy for a common identification standard for federal employees, and contractors. HSPD-12 requires all federal executive agencies and departments to conduct personnel investigations, adjudicate results, and issue a Personal Identity Verification (PIV) or Access Card to all federal employees, contractors, or personnel that require routine or regularly scheduled access to federally controlled facilities, and IT systems. Please visit the GSA Identify, Credentials, and Access Management site for details on how to initiate the credentialing process.

Government sponsors/project POCs need to ensure vendor personnel maintain their ENT accounts and keep them active, to be able to provide technical support going forward. This includes timely completion of all tasks required to keep an ENT account active, such as annual GSA IT Security Training courses and accounts must be accessed at least once every 60 days.

1.3.2 Background Investigations

Per *2100.1P CIO GSA Information Technology (IT) Security Policy* (latest version as of May 2024), those individuals whose duties require a higher degree of trust, such as IT system administrators (or administrative access to building systems server, applications and devices), those who handle financial transactions, or those who deal with PII and other sensitive information (i.e. building drawings, etc.) will require a Tier 2 clearance.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

All access to GSA information systems must comply with the requirements of *2100.1P CIO GSA Information Technology (IT) Security Policy* (latest version as of May 2024). Non-privileged access to a GSA information system categorized at the FIPS 199 High or Moderate level via a network requires Multi-Factor Authentication (MFA), and privileged access to any GSA information system via a network requires MFA.

1.4 BMC Systems Device, Appliance and Software Security Assessment Process

Before any IP-addressable hardware, software or IT device/system is allowed to be connected to the GSA network, GSA IT will need to assess and approve the solution. Any device that is not approved will not have the Authority to Operate (ATO). More information regarding the assessment process can be found in *BMC Systems Security Assessment Process [CIO IT Security 16-76 Rev 4]* (latest version as of May 2024), which is located under IT Security Procedural Guides on insite.gsa.gov.

1.4.1 GSA IT Security Scanning Process

The BMC Security Assessment Team has four types of assessments: Wired, Wireless, Server Software/ Supervisory Control Software (SCS), and BSN Console/Desktop Software. The BMC systems security assessment process applies to Wired, Wireless and Server Software. The process is broken down into six steps: Pre-Assessment, Induction, Assessment, Initial SAR Issuance, Vendor Remediation, and Post-Assessment. ***Please Note: See Section 1.4.4 for the process of BSN Console/Desktop Software assessments.***

1.4.1.1 Step 1: Pre-Assessment

To request a scan, the hardware or software being proposed must be sponsored through an active project. To begin the process, an Assessment Request Form (ARF) must be completed, before the device is shipped to the BMC Security Assessment Team. The assessment request forms must be completed, and all relevant documentation (installation manual, configuration management plan, hardening guide) must be submitted and reviewed before Security is ready to receive the device. The ARF includes instructions on how to submit documentation to the BMC Security Assessment Team. ***Please Note: This form is available to anyone with access to the GSA network. An offline version of the ARF can also be sent to POCs without access to the GSA network.***

The BTSD is responsible for working with BMC systems vendors to identify solutions requiring assessment. Pre-assessment requirements include electrical specifications, technical prerequisites and submitting the required forms. The BMC Security Assessment Team will review the submission and technical specifications to identify compliance with minimum security requirements and accept or reject the BMC systems solution into the BMC Assessment Lab.

The device should be sent configured and hardened as it will be installed on the GSA network (unnecessary ports and services closed, etc.) and be properly assembled for power. The BMC Security Assessment Team is not permitted to work with any electrical wiring, and any device that cannot immediately be plugged into a 110V wall outlet will be delayed (either returned for proper configuration, or on hold until someone can come to the BMC Security Assessment Lab and configure appropriately).

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

The following items are against GSA IT Security policy and best practices:

- No Remote Access (back doors) from outside of the GSA network – access must use GSA provided access (Citrix, Virtual Desktop Interface [VDI], or Government Furnished Equipment [GFE] with Virtual Private Network [VPN]).
- Use of third-party providers (cloud, hosting, etc.) is restricted to only GSA approved and Federal Information Security Modernization Act [FISMA] reviewed third-party providers.
- Protocols such as Telnet, Secure Shell (SSH), Trivial File Transfer Protocol [TFTP] and FTP, Hypertext Transfer Protocol [HTTP], will not be accepted due to the unencrypted nature of the protocols.
- The BMC systems device must not allow changes to security configuration without authentication.
- The BMC systems device must not have hardcoded credentials.
- Use of compromised or weak wireless technology, such as Zigbee (default configuration without any modification), Z-Wave (default configuration without any modification), Bluetooth, 802.11 Wired Equivalent Privacy/ Wireless Protected Access (WEP/WPA) and low-level frequency without protection, such as Global System for Mobile Communications (GSM) Band and Code Division Multiple Access (CDMA) (3G/4G/LTE).
- BACnet will be reviewed on a case-by-case basis.
    - BACnet/Ethernet - Because Layer 2 network traffic cannot be effectively managed on the GSA network between subnets, BACnet/Ethernet is expressly prohibited from being implemented on the GSA Wide Area Network (WAN). BACnet/Ethernet can be used at a given field site, provided all BACnet devices are on the same subnet.
    - BACnet/Internet Protocol (IP) Multicast (B/IP-M) - BACnet multicasting is another way to communicate BACnet messages from one subnet or broadcast domain to another. However, GSA does not allow multicasting over its WAN. Therefore, this approach should not be applied when configuring a BACnet system on the GSA network.
- Windows and Linux based controllers not capable of compliance hardening and monthly OS patching.
- Devices which are not IPv6 capable when connected directly to the GSA switch.
- Server software not capable of utilizing Windows Server 2022.
- BSN console software not capable of utilizing Windows 11.

The following will be needed with each device that is submitted:

- Manufacturer POC
- All relevant information and documentation must be provided to PBS-IT Security, including:
    - Firmware and software versions (these are essential for determining a security baseline)
    - Technical specifications (including information on all inbound and outbound communication on the device, required ports and services, etc.)

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- User Manual
- Installation and Configuration Guide
- Operation and Maintenance Guide
- Configuration/Hardening Guide
- Network diagram detailing network ports, protocols, and services utilized.

- The device and software documentation must provide information related to the system configuration management plan, explaining:
  - How will the device be configured on the GSA network, and how can this configuration be monitored?
  - How will the device be hardened (which ports and services are unnecessary and will be turned off when installed on the GSA network)?
    - All unnecessary ports must be closed.
    - All unnecessary services must be disabled.
  - How will the device be upgraded / patched when updates to firmware or software are released?
- All new contracts with building automation system vendors shall include support language to ensure that security requirements / upgrades will be remediated by the vendor or manufacturer at no additional cost to GSA.
- For wireless technology submissions, include the following information: FCC ID, protocol specification, operational documentation and commissioning guides.

Before shipping the device, make sure the device is configured with the following:

- The device must have sufficient access controls, including:
  - Login screen
  - Password field on the login screen must be masked.
  - Passwords must meet GSA policy strength requirements: passwords must contain a minimum of sixteen (16) characters with uppercase and lowercase letters, symbols, and numbers.
  - Logins must be encrypted.
  - An automatic logout must be configured when inactive for 15 minutes or more.
  - A warning banner on the login screen must be displayed, and configurable.
- The device must be capable of managing user access rights:
  - Least privilege – nobody should have more rights than needed (i.e. a user with a need for read-only/monitoring access should not be able to make changes to the device or the things controlled

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

by the device)

- Documentation should state how user access rights are managed (i.e. administrators, general users, etc.)

- The device must be capable of utilizing TLS (SSL is not sufficient) for the encryption of sensitive data and/or login credentials:
  - Project POC must state what kind of data is being transmitted through these devices (i.e. metering data, energy use data, sensitive data, etc.)
  - Have TLS v1.2 encryption or higher with High Strength ciphers enabled only. Disable SSL v1.0, SSL v2.0, SSL v3.0, TLS v1.0, and TLS v1.1. ***Please Note: TLS v1.3 will become a requirement in the future. Please confirm the latest policy with the BTSD PM.***
  - All web-based logins must utilize TLS v1.2
  - Configured HTTPS to be enabled and HTTP disabled.
  - Enable HTTPS Strict Transport Security (HSTS)
  - Passwords at rest must be encrypted and hashed with AES 256 bit at minimum.
  - Be configured with FIPS 140-2 Compliance (Level 1 at minimum)

- Audit and Accountability (instructions for accessing logs and information detailing what events are audited). The device must be capable of logging the following auditable events:
  - Successful and unsuccessful account logon events
  - Account management events (creation or deletion of user accounts, change in user privileges, etc.)
  - Privilege use events (i.e. administrator functions, changes to or erasure of system logs, etc.)
  - System events (i.e. power failures, lost connection to a server, or other availability issues, system time changes, NTP server synchronizations, etc.)
  - If the device has a web application, the web application must be capable of logging the following auditable events:
    - All administrator activity
    - Authentication checks (i.e. user logons)
    - Authorization checks (i.e. checks of user privileges or access rights)
    - Permission changes (i.e. change in user privileges)

- The device must be capable of being updated:
  - To address code vulnerabilities in the firmware

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- Updates shall be carried out in an offline manner, rather than requiring Internet Access
- All firmware must have integrity checks in place (i.e. Signed packages, checksums, etc.) and only administrators may be allowed to perform the update
- To improve the software or firmware in general ***(Please Note: Major firmware revisions may require reassessment and reauthorization of the device.)***

- If the device uses a Microsoft Windows or UNIX/Linux based operating system, antivirus software must be installed, and a plan must be in place for keeping the AV definitions updated.
- Windows and Linux based controllers must be capable of compliance hardening and monthly OS patching. A patching agreement must be signed by the customer and the vendor.
  - Compliance hardening is based on the NIST US Government Configuration Baseline (USGCB) and must meet 85% compliance or higher.
  - Administrative access is required for GSA to maintain and occasionally perform security validation.
- All devices connected directly to the GSA switch must be IPv6 capable.
  - Addressing must be done at the device level for each NIC and at the application layer.
  - IPv6 addresses must be statically set, via stateless configuration (SLAAC)
- All server software must be capable of utilizing Windows Server 2022.
- All BSN console software must be capable of utilizing Windows 11.
- Any BMC systems device that has 2 or more ethernet ports must provide traffic isolation. Alternatively, if not isolated, provide the ability to disable the port.
- Disable protocols such as Telnet, SSH, TFTP, FTP, MQTT (Only use MQTT-S “Secure”).
- Disable wireless communications unless previously specified as required (802.11 Wi-Fi, Bluetooth, ZigBee, Z-Wave, UHF/RHF, etc.)

Please Note: Any misconfiguration or lack of documentation required by GSA IT may result in delaying the BMC systems security assessment process. Contact [redacted] for any further questions regarding this process. Once IT Security is ready to receive the device, they will provide detailed instructions about shipment.

1.4.1.2 Step 2: Induction

The BMC Assessment Team will attempt to power on, access and establish network connectivity to the BMC systems device.

1.4.1.3 Step 3: Assessment

The BMC Systems Security Assessment Process utilizes a framework to evaluate every type of system (i.e., Building Automation, Lighting Controls, Advanced Metering Solutions, Physical Access Controls

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

systems and/or wireless technology). The assessment process consists of several types of checklists to test all aspects of a solution. It includes testing using automated scan tools to identify any known vulnerabilities at the operating system, web layer, and network layer of the device.

1.4.1.4 Step 4: Initial SAR Issuance

Upon completion of the BMC Systems Security Assessment Process, the BMC Assessment Team will issue a Security Assessment Report (SAR). This document contains all findings and vulnerabilities identified during the assessment, broken down by vulnerability level (Critical, High, Moderate or Low) and recommended mitigations. The SAR will also include the scan reports and the manual assessment checklist attached at the end of the document.

1.4.1.5 Step 5: Vendor Remediation/Final SAR Issuance

All BMC systems solutions are required to go through the remediation process if the SAR is issued with open ‘critical’, ‘high’, or ‘moderate’ findings. The BMC Assessment Team will distribute the initial SAR to the BMC systems vendor and appropriate PBS stakeholders with a review meeting is held to go over the findings and provide guidance to the vendor for remediation or mitigation of the findings. The vendor is responsible for addressing the identified vulnerabilities. ***Please Note: The resolution of the findings is ultimately at the discretion of the vendor to address or reject. Based on the vendor’s priorities this process could take time to remediate (i.e. months to years).***

Once the vendor reviews the SAR, they will provide their remediation plans. This could include documentation updates, a firmware update, or a software update. The BMC Assessment Team will verify the remediation plans and ensure that it meets the security requirements. Once the update is provided, the BMC Assessment Team will install the update and re-scan. If the remediation scan comes back free of vulnerabilities, then the BMC Assessment Team can mark the product as Remediated and issue the Final SAR. If the remediation plan does not adhere to the security requirements, then the BMC Assessment Team has the right to reject the product and mark it as non-remediated. If a BMC systems component is identified as non-remediated, GSA is prohibited from being on the GSA network. The status of each product will be displayed on the Device Scanning Dashboard (AN-RR Dashboard).

The BMC Final SAR is a snapshot in time, whose results lose relevancy over time as new vulnerabilities and exploit techniques are identified. The SAR validation is for three years and after this expires, a re-scan is required.

1.4.1.6 Step 6: BMC Systems Service and Support

It is the responsibility of the PBS Business Line to ensure a service support contract is in place to support any additional remediation or upgrades to the device. If the device undergoes changes as a part of the System Development Life Cycle (SDLC) process, or has an identified security incident, there may be a need to reassess the device/SCS.

In the production environment, if a device or software has a new vulnerability discovered, the vendor must provide a patch. If a patch is not available yet, the vendor must provide a remediation plan and the project POC must request an Acceptance of Risk (AoR) from the Authorizing Official (AO) to accept the risk that the device/system would impose on the GSA network. Once the patch is provided, the PBS Business Line must apply the patch per the timelines below.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

GSA Standard Timelines

- Within 30 days for Critical (Very High) and High vulnerabilities.
- Within 90 days for Moderate vulnerabilities.
- Within 120 days for Low vulnerabilities for Internet-accessible systems/services.

Binding Operational Directive Timelines

- Remediation within 14 days for vulnerabilities added to CISA's KEV Catalog with a CVE date post FY21.
- Per the CISA KEV catalog date or GSA Standard timelines above, whichever is earlier, for vulnerabilities in the CISA KEV catalog with a CVE date in FY21 or earlier.
- Within 15 days for Critical (Very High) vulnerabilities for Internet-accessible systems or services.

Please Note: For any BMC systems device that is a Windows or Linux based Operating System, the PBS Business Line is responsible for having a signed agreement between the vendor and GSA adhering to patching monthly. The vendor will be responsible for patching the devices.

1.4.2 Wireless Assessments

GSA IT Security will need to evaluate non-IP wireless devices due to the higher level of threat they pose. Wireless technologies must have a minimum level of AES 256-bit encryption, with the only exception being Zigbee, which currently does not support AES 256-bit encryption. All 802.11 solutions must adhere to the *2100.2C CIO GSA Wireless Local Area Network (WLAN) Security* guide before they can be connected to the GSA network. Additionally, other non 802.11 wireless solutions are required to be scanned, remediated, and the solutions evaluated and approved by GSA IT Security in advance of any implementation.

Use of compromised or weak wireless technology results in broken encryption that can be exploited to leak sensitive information and are not permitted. These include:

- Zigbee (default configuration without any modification),
- Z-Wave (default configuration without any modification),
- Bluetooth (less than v4.1),
- 802.11 Wired Equivalent Privacy/ Wireless Protected Access (WEP/WPA)
- Low level frequency without protection, such as Global System for Mobile Communications (GSM) Band and Code Division Multiple Access (CDMA) (3G/LTE)

Wireless connections can be permitted with the following requirements in place:

- **802.11 Requirements:**
    - Infrastructure Mode (BMC systems device to BSN Infrastructure): All new GSA wireless LAN implementations must meet 802.11i requirements for encryption using the Counter Mode with CBC-

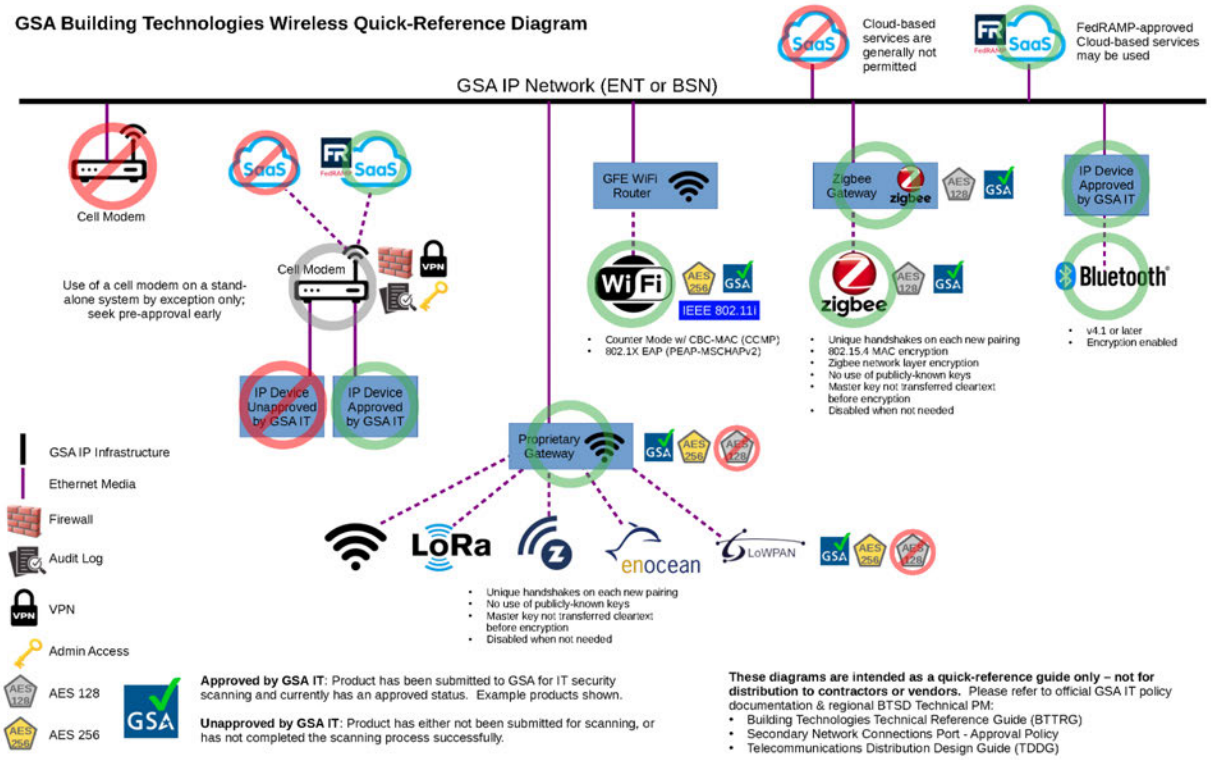
DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

MAC (CCMP) protocol and AES as its encryption algorithm. In addition, it must use 802.1X port-based network access control for authorization and authentication (EAP). The EAP authentication mechanism that must be used is Protected EAP (PEAP- MSCHAPv2).

- Ad-hoc Mode (Device to Device): Any BMC systems device to BSN console or other BSN peripheral, must have the ability to utilize WPA2-AES 256-bit at minimum.

- **ZigBee Requirements:**
  - AES 128-bit level encryption is implemented.
  - Each new pairing requires a unique handshake.
  - The 802.15.4 Medium Access Control (MAC) Layer is encrypted.
  - The ZigBee Network & Application Layers are encrypted.
  - The vendor has not implemented any publicly known encryption keys.
  - The master key is not transferred over Cleartext before encryption.
  - ZigBee will be disabled when not needed.
- **Proprietary RF (6LoWPAN, LoRa, Z-Wave, ISM band, etc.) Requirements:**
  - AES 256-bit level encryption is implemented.
  - Each new pairing requires a unique handshake.
  - Proprietary RF will be disabled when not needed.
- **Bluetooth Requirements:**
  - Devices must use the Bluetooth Protocol version 4.1 or later.
  - Encryption must always be enabled for Bluetooth connections (i.e. "Security Mode 1" does not enable encryption, and therefore should never be used).

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514



1.4.3 Encryption

The Federal Information Processing Standard (FIPS) 140-2 is a U.S. government computer security standard used to accredit cryptographic modules, which is necessary in order to maintain the confidentiality and integrity of the information system. Once a system has been designed and deployed using FIPS compliant technologies it must be operated following documented procedures to ensure keys are created, stored, retired, revoked, and otherwise managed in a consistent and secure manner. All file/data transfers inbound to or outbound from the device or software must be encrypted using FIPS 140-2 compliant protocols, as well as machine-to-machine transfers.

1.4.4 Non-Standard Software Review Process (BSN Console Software)

Non-standard software refers to applications that are not readily available on standard images on a GSA workstation, or software that is not yet listed as approved on ServiceNow (GSA's enterprise ticketing system). All non-standard software, that has not yet been assessed by GSA IT, will need to complete the evaluation process. GSA IT performs an assessment of the non-standard software, which focuses on ensuring software is currently supported, is 508-compliant and is generally secure and free of vulnerabilities.

To start the evaluation process, submit an Assessment Request Form (ARF) from the PB-ITS InSite page. The BMC Assessment Team will reach out to collect the software installation package(s) and relevant documentation. The status can be tracked via the AN-RR Dashboard. Projects need to ensure that only approved software is installed on GFEs, including the BSN consoles.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

1.4.5 Variable Refrigerant Flow (VRF) in HVAC Controls

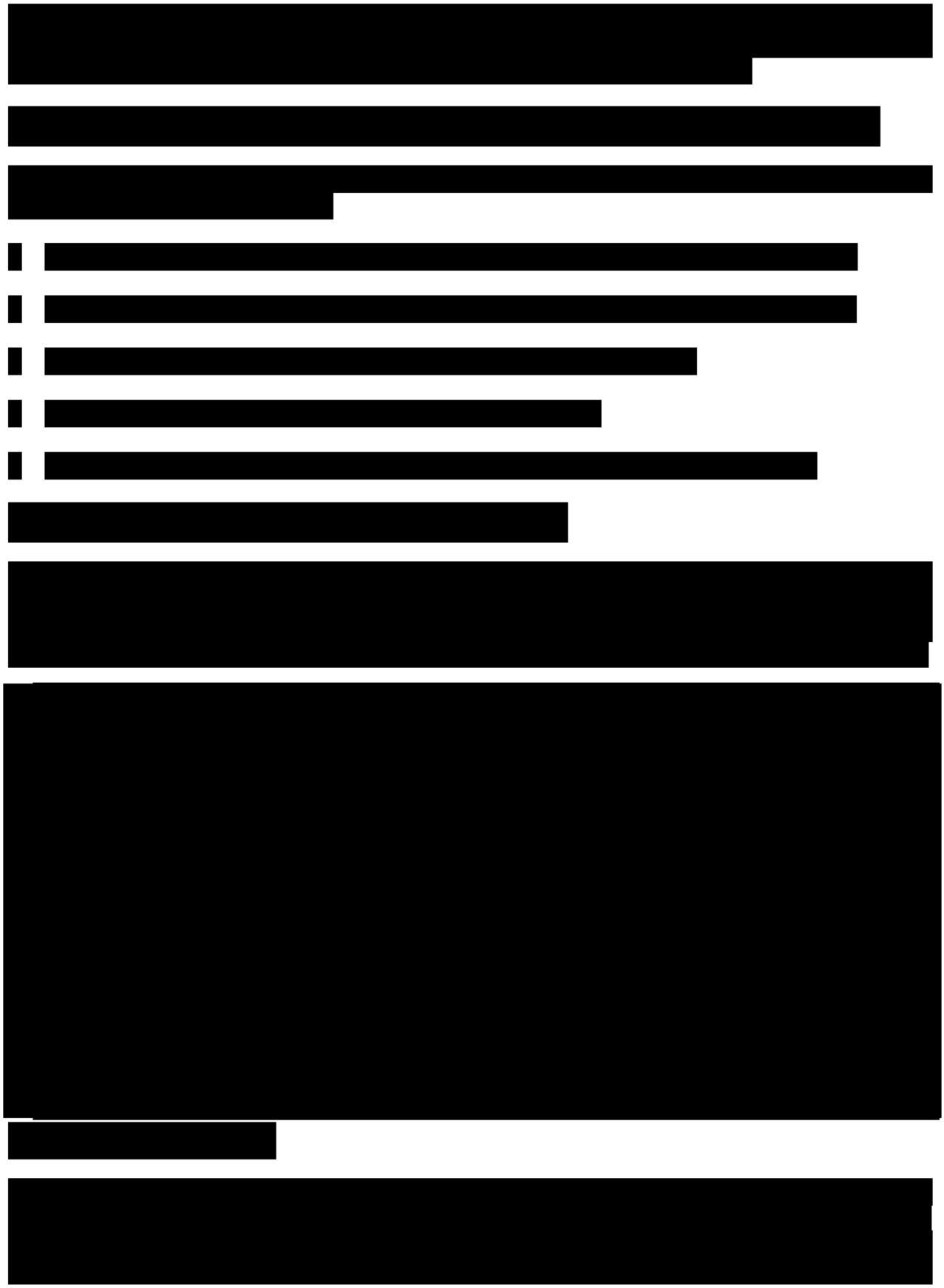
VRF Systems are inherently very proprietary and the main vendors (e.g. Trane, Mitsubishi, etc.) have been historically unwilling to participate in the GSA IT remediation process. Additionally, any second-tier communication over BACnet or through a Gateway is not an option due to the open protocol interface of these devices limiting the exposure of important data points and control features.

Because of the challenges GSA cannot connect their systems directly nor through second tier communications. These systems can only be operated in stand-alone, island mode, which limits operational monitoring and control of these systems for the long term.

In addition, due to OFM and GSA IT concerns related to useful life of VRF systems, total cost of ownership, carbon/refrigerant emissions, and risk factors that could impact life safety the following minimum requirements for use or incorporation of a VRF's are:

- The VRF must be connected to the building BAS system.
- The VRF proprietary controller must pass GSA PB-ITS security scanning and be fully remediated.
- The controls must be native BACnet, and we must be able to get into the controls not only to monitor but to control.
- The list of connected points specifically for VRF systems must be those in the GSA Data Normalization for Building Automation Systems, Version 2.5, Appendix C, Sheets 48 through 50. All the listed points must be provided for remote monitoring and control.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514



DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

[redacted]

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

1.5.4 Steps to Integrate Sites onto the BSN

The GSA requires all new sites to be integrated into the BSN. However, older integrated sites still exist on the ENT domain and will need to migrate over to the BSN as soon as that becomes possible. To accomplish this endeavor there are several steps and tasks that must be completed for a successful migration. Below are the steps and tasks needed to accomplish this. All steps will be coordinated by the BTSD IT PM.

- Are the BMC systems devices remediated and approved to be placed onto the GSA network?
    - Yes - Move onto the next step.
    - No - There must be a project in place to upgrade all BMC systems devices to meet GSA IT security requirements. ***Please Note: See Section 1.4 for details on how to submit new devices to the BMC Assessment Team.***
- Is there a GSA network onsite?
    - Yes - Move onto the next step.
        - Verify the location currently operates on a subnet compatible with BSN, which is the Class B [redacted] range. If the site does not operate on this or a valid range, then the regional BTSD IT PM will submit a ServiceNow “New Circuit Request” ticket within ServiceNow for a new IP range.
    - No - Request a new GSA circuit via the Network Team ***Please Note: See Section 2.4.2 for details on how to order a GSA circuit.***
        - Once the GSA circuit is added to the site, the regional BTSD IT PM will submit a ServiceNow “IP Address Request” ticket for a new IP range.
- The contractor and/or property management will need to ensure the cables for the network are in place and in accordance with GSA IT requirements before the BTSD IT PM can order switches. ***Please Note: See Chapter 3 for cabling requirements.***

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- The BTSD IT PM will determine the necessary amount of GSA switches for the integration project. They will submit a ServiceNow “Switch Request” ticket for new network switches.
- The BTSD IT PM will submit a ServiceNow “VLAN Change/ISE Exception Request” ticket to “whitelist” the devices that will be connecting to the network.
- The BTSD IT PM will provide the static IP, subnet, and gateway information to the O&M contractor/project integrator to implement the device configuration settings.
- The BTSD IT PM will submit a ServiceNow “GSA Workstation” ticket for a BSN console. They will ensure that the BSN console has the correct configuration and all software necessary to operate the building.
- All building staff and those requiring access to BSN will need to have Citrix VDI accounts and confirm access to the “PBS Building System Desktop” within Citrix VDI prior to BSN cutover. ***Please Note: See Section 4.5 for further information on how to access the BSN via Citrix VDI.***
- The SBS team will determine which shortcuts are needed and then help create an RDP shortcut in the “BMC RDP Shortcuts” folder within Citrix VDI. Then, the SBS team will need to train facilities management/O&M personnel on accessing BMC systems via BSN Console or Citrix VDI.
- For sites that rely on DNS, the BAS navigation will need to be updated with the removal of any DNS entries for it to operate effectively on the BSN.
- The BTSD IT PM will coordinate with the O&M contractor/project integrator and GSA IT security on implementing TrustSec enforcement mode.

1.6 Incident Response (IR) and Building Recovery (BR) Exercises

Since IP addressable BMC systems reside on the GSA network, they are subject to interruptions in service. In the event of a data circuit failure, Local Area Network (LAN) outage, cyber-attack or application server failure, GSA facility managers and O&M staff must be prepared to operate the facility locally.

1.6.1 Incident Response

An incident is defined as a violation or an imminent threat of violation of information security or privacy policies, acceptable use policies, or standard security practices. An IR entails the contractors’ ability to identify a potential cyber incident and immediately report the issue to GSA IT [redacted] For additional questions, please reach out to the regional BTSD IT PM.

1.6.2 Building Recovery Exercises

A properly developed BR plan will ensure that while network communications may be temporarily unavailable, building control system components will continue to function (i.e. in the event of a LAN or WAN outage, all sites need to make sure the controllers have a set default setting programmed, and have an ability to directly connect to the controllers to manage the system manually). A designated facility POC will be required to document and submit operational procedures to monitor and control systems in case of an outage. To make the documentation process easier, please reach out to the regional BTSD IT PM for a copy of the BR Exercise template. Once the documentation is completed, please reach out to the BTSD IT PM so that they can submit a ServiceNow generic ticket for an outage simulation. Executing the BR exercise

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

will require coordination and participation from Facility Management, O&M, the regional BTSD IT PM and, if applicable, the integrator. At the start of the BR exercise, the BTSD IT PM will simulate the outage. Then, the O&M will need to follow the BR procedures to ensure continued operation of the system. When the operation of the system is confirmed, the network connection will be re-established, and the O&M will provide a written summary of their findings. The findings should include any necessary updates to the procedures and/or lessons learned. ***Please Note: It is strongly recommended to add BR exercises to any new projects/ contracts. For language on how to include BR exercises into the Scope of Work (SOW), please see Chapter 9 for more details.***

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Chapter 2

Network Infrastructure

2.0 Overview

A network can be defined as a collection of interconnected devices that facilitate communication among a set of users or devices, allowing them to share hardware, software, resources, and information. Networks use a variety of protocols to organize and communicate data amongst the devices connected to that network. Primarily, an ethernet-based network, which supports the TCP/IP protocol, is used to form an inter-building or site network. Other intra-building networks can be used to connect devices within a facility (i.e. BACnet). Wired technologies include Cat5e (if adding to existing infrastructure), Cat6 (all new cabling), and optical fiber cable. There are two main geographically based configurations for ethernet networks. A Local Area Network (LAN) is a network that connects computers and devices in a limited geographical area such as an office building, or a closely positioned group of buildings (i.e. campuses or border stations). A Wide Area Network (WAN) covers a large geographical area such as a city, or a country. GSA's WAN connects all the regional office buildings, field offices and data centers together onto an enterprise network.

This chapter will focus on networking protocols, specifically TCP/IP (used to form an inter-building network) and BACnet (a data communication protocol for building automation and control networks). It will define acceptable network topologies, standards for interconnection with the GSA network and the process by which network designs will be approved.

2.1 Network Roles and Responsibilities

- **GSA IT Building Technology Services Division (BTSD):** The BTSD is responsible for all information technology systems within PBS and facilitating the review and approval of network design diagrams.

- **GSA IT Network Operations and Management Team (Network Team):** The network team has command responsibility for the GSA Wide Area Network (WAN) and Local Area Network (LAN). They are responsible for the entire IP transport layer and are the sole provider for IP/subnet allocation at the building level. In addition, they manage network devices (i.e. routers and switches) and the BSN's connectivity. ***Please Note: PBS is responsible for the controllers/devices. GSA IT provides connectivity up to the switch port.***

- **GSA IT Security Operations Team (SecOps):** The SecOps Team provides network security management for GSA infrastructure to include firewalls, intrusion detections and virus detection systems.

- **Office of Facility Management (Facility Managers):** The facility managers are responsible for securing network equipment properly in GSA-owned IT spaces. They are also responsible for funding and managing the installation, maintenance and repair of cabling and switch cabinets or brackets.

- **Vendor/Contractor:** The vendor/contractor is responsible for adhering to GSA IT policies. This

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

includes a GSA network riser diagram. ***Please Note: See Section 2.4 for details about network diagram requirements and submission.***

2.2 Standards for Interoperability

The following information will cover the standards for interoperability for all BSN/BMC Systems.

- All new networked federal BMC systems must be IPv6 capable. The intent is to phase out IPv4. ***Please Note: As of July 2023, IPv4 will no longer be allowed for new projects/assessments. Devices communicating via secondary tier communications or native protocol (i.e. BACnet/MSTP, Modbus/MSTP, etc.) are not impacted.***

- Only GSA-furnished equipment (GFE) hardware is permissible (i.e. routers, switches, servers, and workstations) for BMC integrated systems. Vendor-provided intermediary devices such as media converters, hubs, switches, and routers on the GSA network. GSA IT switches are configured to detect and disengage with such devices on the network.

- Where possible, utilize an existing switch to support all approved agency hardware, including ENT user workstations, printers, BMC systems devices, BSN consoles, etc. Additional switches will be provided to accommodate new projects if the existing switches are inadequate (i.e. port saturation, distance, etc.).

- Switches should be connected using the assigned trunk port only.

- When adding a new switch, there must be a dedicated power source.

- All cabling must meet the latest Telecommunications Distribution Design Guide version 8 requirements (latest version as of May 2024).

- All Ethernet (IP enabled) devices need to terminate at a GSA switch.

- All IP enabled devices, prior to deployment, will be subject to scanning and certification. ***Please Note: See Section 1.4 for details on the BMC Systems Security Assessment Process.***

- All whitelisted devices must connect to a GSA switch. ***Please Note: See Section 1.2.3 for details on the BMC Device Whitelisting Process.***

- BMC systems devices shall not be plugged directly into workstations or servers for daily building operations.

- Data collection shall only be done on systems classified and operated as servers and not workstations.

- Per the *P100: Facilities Standards for the Public Buildings Service* (Latest is version 1 as of May 2024): “Except for mass notification, a fire alarm and emergency communication system are not permitted to be integrated with other building systems such as building automation, energy management, security, and so on. Fire alarm and emergency communication systems must be self-contained, standalone systems able to function independently of other building systems.” As such, GSA IT does not provide UL switches. However, the new Fire and Life Safety SOP for dual path communicators requires that the communicators (e.g. Bosch 465) be connected to the GSA Network. The primary line will utilize a

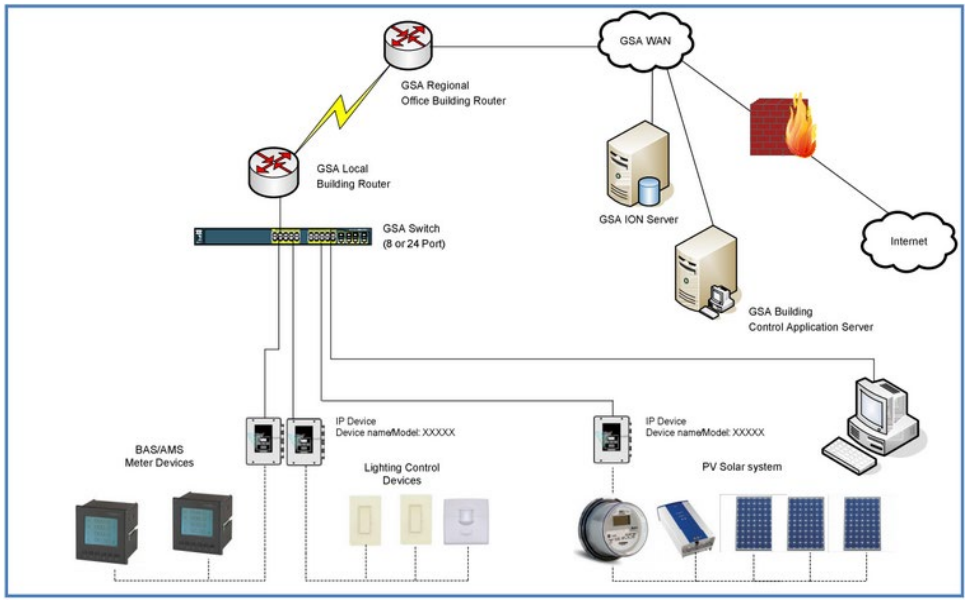
DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

GSA Network switch to relay out the alarm to the third-party monitoring station and cellular connection as the back-up or fail over means of relaying the alarm. The dual path communicator must be remediated and approved in the same manner as all other BMC systems devices.

- Per the *ASME A17.1-2022/CSA B44:22: Safety Code for Elevators and Escalators* (latest version as of May 2024), a new emergency communication system has been mandated. The new code requires video transmission in the event of an emergency. As such, the system will need to be connected to the GSA Network and the BMC Systems Security Assessment Process for connecting devices to the BSN applies. Reach out to your BTSD PM or Regional Elevator SME for more information.

2.3 Network Topology

The following figure is a topology that demonstrates an example of interconnections between GSA WAN and LAN and the vendor-provided devices. This example provides a foundational approach for the design of an integrated building controls and/or energy system.



2.3.1 Network Design Requirements

These are the following items that need to be addressed in the proposed network diagram sent to the GSA IT Network Team:

- Location of Demarc Room
- Location of Demarc Extension Room (if applicable)
- Location of Router
- Cabling:
    - Switch to switch connections and the type of cable being used. Minimum standard for Ethernet is plenum-rated, Unshielded Twisted Pair (UTP), Cat5e (if adding to existing) cable. Any new cabling

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

requires Cat6, certified RJ45 (M/F) and patch panels.

- Depict cable home runs from access layer switches to the core/distribution switches. In the instance that it is cost prohibitive or not feasible, daisy chaining may be allowed based on the Network Team's discretion. If needed, the daisy chained switches must not exceed a maximum of three (3) hops from the core/distribution switch. ***Please Note: The facility or project manager must sign off on risk associated with daisy chaining. If a switch fails, it may cause a ripple effect on switches that are daisy chained to it.***
- For any fiber optic cable runs, detail the type of fiber, single mode or multimode, shielded, or armored, and the type of connector (ST, SC, FC, MT-RJ, & LC).

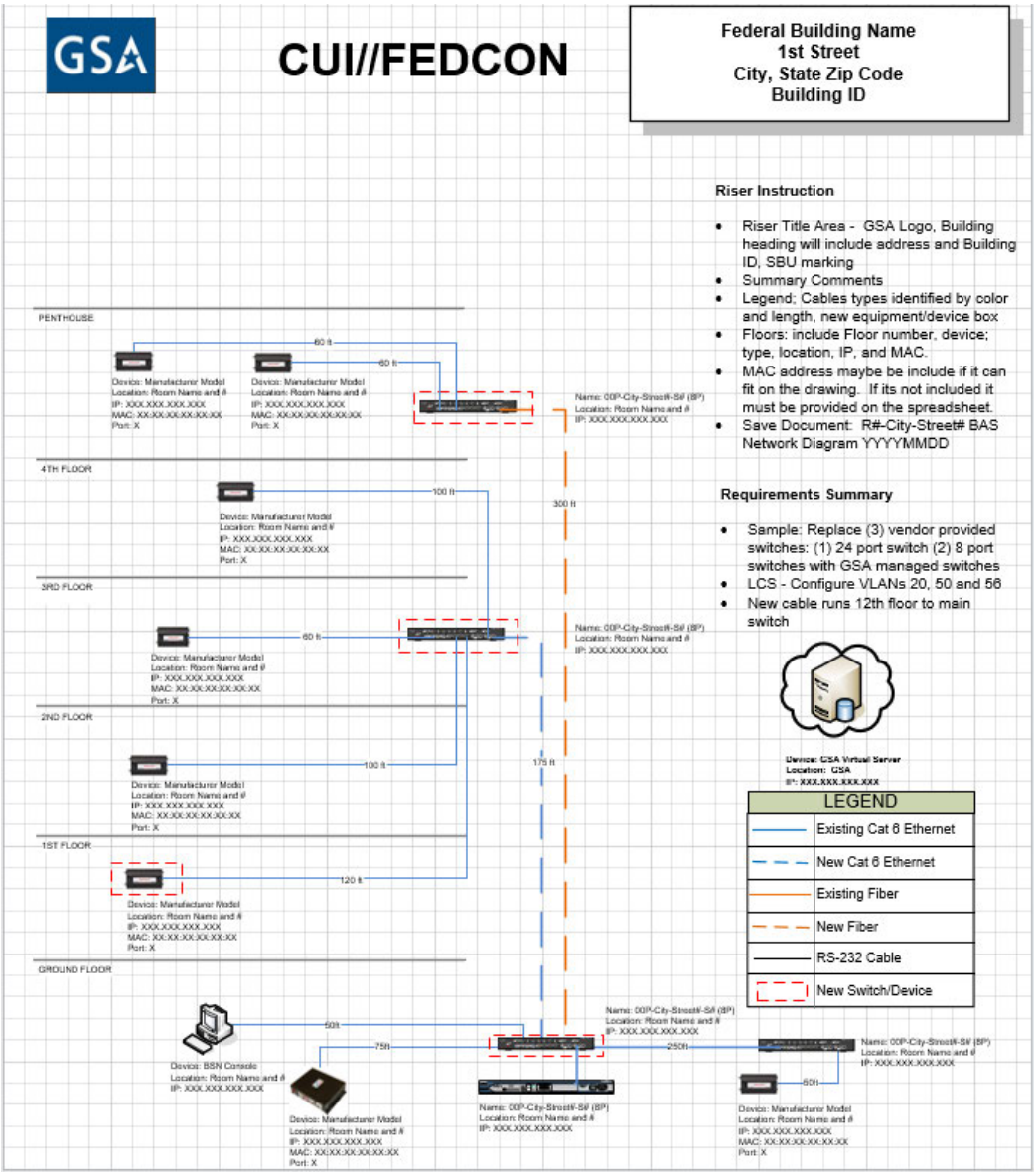
- Switches:
  - Location of switches (building ID, floor, and room numbers) ***Please Note: It is not necessary to deploy a switch on every floor. Hardware from adjacent floors can be connected to switches on adjacent floors, provided it is within the attenuation limitations maximum distance of 300 ft.***
  - Port density requirements for every deployed switch
- IP-Addressable Devices (each device requires the following information):
  - Manufacturer
  - Model
  - Firmware
  - MAC address
  - Switch and port number the device will connect to
  - Location of Device (building, floor, and room numbers)
  - Cable length between device and switch
  - In the instance a secondary NIC architecture is approved, the vendor must provide a network diagram of all downstream devices, including all types of cabling. ***Please note: See Section 2.4.5.2 for more details on the different types of alternate connections.***
- Controlled Unclassified Information (CUI) Federal Employees and Contractors (FEDCON) notice must be included on the top right hand corner network diagrams.

CUI//FEDCON

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

2.3.2 Sample Network Design Diagram

The following is a sample depiction of an acceptable network design diagram. The diagram illustrates all the requirements mentioned above. The vendor will need to provide an acceptable network design diagram to the GSA IT before any hardware is sent to the project. Please work with the BTSD Technical PM and RBITS to have the network design diagram reviewed by the Network Team.



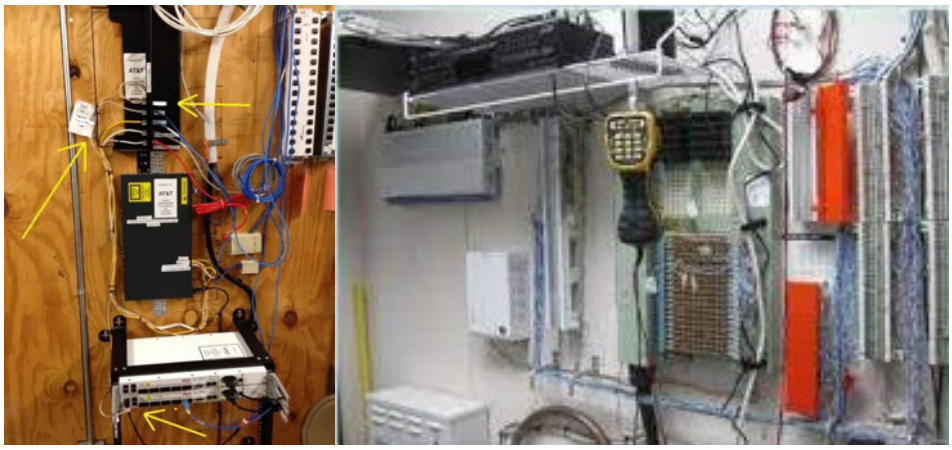
2.4 Requesting and Installing a GSA Circuit

This section will cover the steps of how to locate the demarc room and the demarc extension room, how to request a GSA circuit and the installation process, and important considerations for installing a GSA circuit.

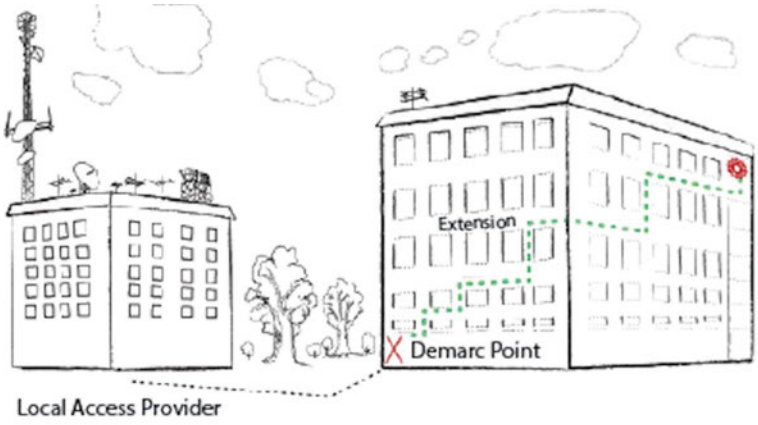
DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

2.4.1 How to Locate the Demarc Room and Demarc Extension Room

The demarc room and demarc extension room need to be located before requesting a new GSA circuit. The demarc room, also referred to as the main point of entry (MPOE), is the physical location where cable/phone companies bring their service into the building. The room may look like the photos below. You might see boxes from carriers like AT&T or Verizon if another agency already has a network in the building.



The demarc extension is the end point where the service needs to be extended to in the building, which is also where the router will need to be located. The room is usually in an office, or it may be close to where a building automation/metering system will be installed. The demarc room and demarc extension room will need a cable run installed between the two points.



2.4.2 How to Request a GSA Circuit and the Installation Process

Before any project begins, the project sponsors/POC must reach out to the BTSD IT PM to see if a GSA circuit exists at the site. If not, they must work with the BTSD IT PM to order a GSA circuit before starting the migration project. The circuit installation or upgrade process typically takes anywhere from three months to a year from the day that the order is submitted by the Network Team to Mettel (not when the ServiceNow ticket is submitted). Potential delays include, but are not limited to location of site, onsite personnel not available to escort, construction activities required by the provider, etc. To submit a request for a circuit, the government sponsor/project POC must:

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- The BTSD IT PM will submit the ServiceNow “New Circuit Request” ticket on the customer’s behalf. The information needed will be:
    - Building Code
    - Exact Building Address (the building that the circuit will terminate in)
    - Demarc Room
    - Demarc Extension Room
    - Estimated Distance between Demarc Room and Extension
    - On-Site POC (Name, Phone Number(s), and Email)
    - Total # of Users
    - Number of Users Per Floor
    - Power over Ethernet Required?
    - Wi-Fi Requested?
    - BSN Required?
    - Customer Wanted Date
    - Application List
    - Telephone number that is in the building where the circuit will terminate (not a cell phone but a landline)
    - Requirements if users will be supported by the circuit in addition to the BMC systems.
- The Network Team will schedule a call with the local on-site POC to validate all information provided.
- The Network Team will request Mettel to add the site to the contract.
- The Network Team will submit the new order to Mettel.
- Mettel will then get an NSC code, which is an identifying code for billing. Then, once the NSC code is created, it will need to be added to the contract as a task order. This process can take anywhere from one to two months.
- Once the NSC code is added to the task order, the Network Team can place an order for a new circuit.
- Once the order is placed, Mettel hires a local vendor who works with the on-site POC to do the installation and construction of the project. Sometimes this process can take anywhere from one to six months, depending on how much work needs to be done. Fiber is not always readily available at a site and a contractor would need to be hired to extend the fiber to the building.
- Once the installation is complete, DIGIT will set up the prep calls.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- Once the circuit is installed, DIGIT works with the site to schedule an activation date/call. Based on the availability of the provider tech and the site, this step can take up to one month.

Please Note: Although the BTSD IT PM submits the "New Circuit Request" ticket on your behalf, the Network Team is responsible for ordering the circuit and deploying it on the customer's behalf. For any status updates, issues, etc. please reach out to the Requirements Analysis Team [redacted]

2.4.3 Important Considerations in the Circuit Installation Process

Proper design and placement of the circuit and router are paramount for a successful and on-time project completion. This is especially important during the design phase to avoid having to move the circuit from the location where it was initially ordered. Circuit moves based on a mistake, from other than the telephone vendor, will incur additional charges that will be passed on to the project and will extend the delivery time of the completed circuit. A good address for the site location is also critical in this process. A physical address is not always the same as the telecommunications address. A good address is an address verified from the postal service website or Google Maps. A carrier will not accept a non-specific address and will cause delays in the installation timeline.

2.5 Hardware Standards and Policy

This section will cover the configuration and connection of switches and routers, and standard and non-standard hardware connectivity options. ***Please Note: The Network Team does not provide any hardware necessary to mount the switches and routers in place. The local site needs to provide and install all items necessary to mount the hardware, such as cabinets, shelves, etc.***

2.5.1 Requesting and Installing Switches

Once the network diagram is approved and the site's GSA circuit availability is confirmed, the project sponsor/POC will need to work with the BTSD IT PM to coordinate the ordering, delivery, installation, and connection of the switches. Before any switches are ordered, a POC, date and time for installing and connecting the switches must be determined. Once the information is confirmed, the BTSD IT PM will submit a ServiceNow "Switch Request" ticket on behalf of the project sponsor/POC. A switch request for 1-2 switches may take up to two weeks from the date the BTSD IT PM submitted the ticket. Switch counts exceeding that will be determined on a case-by-case basis. The preferred POC to install the switches is either a POC onsite or the cabling vendor. If neither are viable options, BTSD IT PM will work with the Network Team to dispatch a SmartHands technician at an additional cost. ***Please Note: Emergency requests (replacements/failures) are addressed by the Network Team.***

2.5.2 Installing and Connecting Hardware

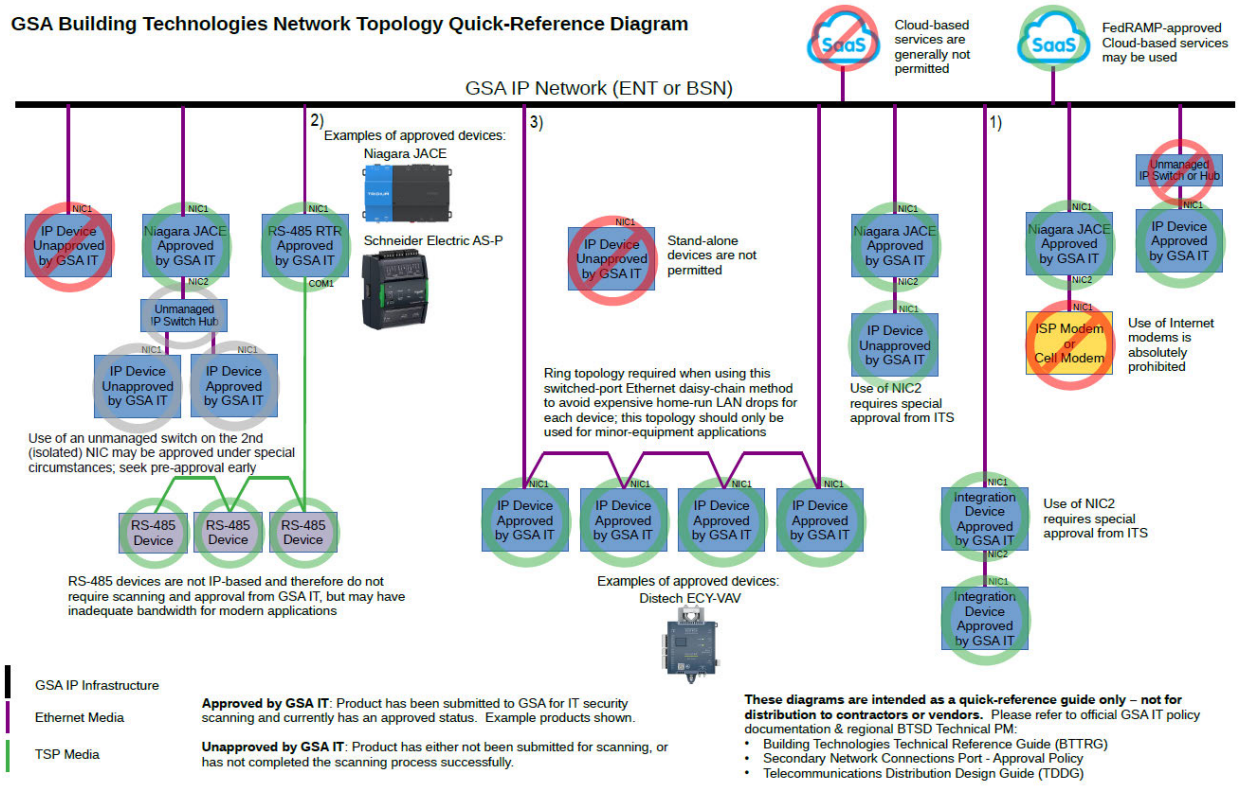
All hardware designed for implementation must be scanned and approved by the GSA IT Security Team prior to implementation. Once the devices are cleared to be put on the network, the BTSD IT PM will submit a ServiceNow "VLAN Change/ISE Exception Request" ticket. This will change the VLAN for designated ports on the switches to the correct BSN VLAN as well as "whitelist" the devices to allow communication to the GSA BSN network. It is imperative that this ticket is resolved prior to physically connecting the devices onto the network. If a device is physically connected prior to being whitelisted, the site risks the port on the switch locking down and not allowing any communication. ***Please Note: See Section 1.4 for details on***

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

the BMC Systems Security Assessment Process.

2.5.2.1 Types of Connections Allowed

The following figure shows the approved network topologies that are or are not allowed on the BSN or ENT. ***Please Note: The gray circled scenarios can be approved by BMC-IT Security on a case-by-case basis.***



2.5.2.2 Alternate Connectivity Options for Approved BMC Devices

Building Management Controls (BMC) system devices have expansion ports onboard that offer a great deal of flexibility. However, GSA IT Security has frowned upon its usage and in some cases prohibited their use. This guidance is being created to bring forth common situations where these ports may be necessary for business operations and allow for exceptions to the guidance.
The following scenarios are examples of common usages for each technology:

- **Secondary Network Interface Card (NIC)** - BMC IT Security will **only** allow the use of the 2nd NIC when the device has been reviewed and approved through the assessment process. Devices that wish to be connected to the 2nd NIC can be remediated, un-remediated, or have never gone through the lab as long as the 2nd NIC is not visible from a GSA switch and can only be visible via the “master” device (which is remediated). Currently there are two main networking architectures for the 2nd NIC:
    - Switched networking (all traffic on the 2nd NIC is shared between the primary NIC)
    - Isolated networking (all traffic on the 2nd NIC is hidden and completely segregated)

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- **Serial Ports (RS-232, RS-422, RS-485)** - Used for connecting End of Life (EoL) devices, Remediated devices, non-remediated devices, and devices which have not gone through the assessment review process or do not have/are not utilizing an IP based connection by which they may be assessed. Serial MSTP connections do not require GSA IT approval.
- **Universal Serial Bus (USB)** - Used for updating the firmware, exporting data, terminal shell access, external display output, troubleshooting, and non-routine maintenance.
- **Spanning Tree** - Daisy Chaining is connecting (several like devices) together in a linear series over an ethernet connection. Connecting devices in a daisy-chain fashion is prohibited on the GSA network. Spanning Tree Protocol (STP) is a Layer 2 network protocol used to prevent looping within a network topology. Other common configurations include Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP).
    - As of May 2024, GSA continues to research and collaborate with Cisco and multiple BMC systems vendors on the implementation of RSTP (or similar). GSA will continue to utilize MSTP while this research continues.
    - Per an internal memo released in July 2023, all GSA projects will continue to utilize MSTP unless the contract has been awarded and the installation is underway. If that is the case, then the following need to occur:
        - The maximum number of devices in a “chain” is limited to seven with the maximum number of devices allowed on a Cisco 9300 (C9K) is eighty-four.
        - All loops must start and end on the same switch. NetOps has indicated that only the Cisco 9300s switches are allowed to utilize RSTP Loop. ***Please Note: Connecting devices in a RSTP fashion using an ethernet connection will require additional configuration on the switch. The BTSD IT PMs need to submit a request ticket for this step to the BMC ISSO and NetOps for approval. Validation of network hardware is required to ensure any of these solutions will be supported.***
        - Ticket to NetOps needs to note:
            - RSTP Loop Configuration required (support authentication for multiple MAC addresses on the switch)
            - Configuration for loop devices, remove Spanning-tree PortFast command, and add authentication mode multi-auth to specific loop interfaces.

2.6 BACnet

BACnet, by definition, is a "Data Communication Protocol for Building Automation and Control Networks" developed by the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). BACnet is neither software, hardware, nor firmware. BACnet functions as a standardized set of rules that governs how computers exchange information. These rules enable the integration of control products made by different manufacturers into a single, cohesive system. While it is first being used in HVAC applications, the BACnet standard is designed to support other building control systems such as life safety, security, and lighting. ***Please Note: While we prefer BACnet SC (secure), we will still accept legacy BACnet (insecure) connections.***

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

2.6.1 How Does BACnet Make Use of IP Networks?

For BACnet to utilize the Internet for communication, it must speak the language of the Internet known as Internet Protocol (IP). IP by itself is little more than an envelope with a "from" and "to" address and a place for a message within. For equipment to communicate on the Internet a second transport layer protocol must also be used. Currently there are two primary transport layer protocols, "Transmission Control Protocol" or TCP and "User Datagram Protocol" or UDP. TCP is a reliable connection-oriented transport service that provides end-to-end reliability, re-sequencing, and flow control. Simple analogy: TCP/IP is like a telephone call providing means of communication between two parties and BACnet is the language being spoken between the two parties. UDP is a connectionless "datagram" transport service. It is used by applications that do not require the level of service of TCP, provide the same services, or that wish to use communication services not available from TCP such as multicast and broadcast delivery. Since the BACnet protocol itself provides for the guaranteed delivery of packets, re-sequencing, and flow control, it does not require the use of TCP and therefore utilizes UDP. UDP/IP was added to the BACnet specification first in Annex H.3 and later with Annex J and requires specific devices or services to be available on the BACnet network.

2.6.2 BACnet Key Definitions

- **BACnet Object:** The general reference to sensors, actuators, and other functional elements that make up a BACnet device. The objects fall into categories specified by BACnet protocol. Analog Input object and Analog Output object are a couple of the most used objects

- **BACnet Device**: Any device, real or virtual, that supports digital communication using the BACnet protocol. Data inside a BACnet device is organized as a series of BACnet objects. Each object has a type and a set of properties. There is always at least one object in a device that is used to represent the device itself.

- **Device Instance:** This is the logical address that matters to BACnet. Whether on an MS/TP link or IP network, the device instance for a particular BACnet system must be unique across all subnets and routed links. There are over 4 million possible unique device instances based on the BACnet protocol.

- **BACnet Broadcast:** A message sent as a single unit, which may apply to more than one device.

- **Broadcast Domain:** This is the collection of available BACnet objects that can be reached by a broadcast message. With respect to IP, it is analogous to the IP subnet that one or more BACnet devices reside on. For example, in GSA, each field site may have one IP subnet that each of its building control devices resides on. A BACnet broadcast from a device on that subnet cannot communicate via a BACnet broadcast to any other BACnet device on a different IP subnet. It would require direct communication from a BACnet Router or BACnet Broadcast Management Device (BBMD) as described below.

- **UDP/IP:** The UDP side of the stack operates in parallel to TCP and is automatically included in most implementations of an Ethernet based protocol stack. TCP is considered a "connection" protocol, and all communication takes place in a session that has overhead to ensure delivery of all packets. UDP is considered "connectionless", has minimal overhead, and allows the application to deal with whether the packets were delivered or not. is used when data efficiency and latency is important and not data integrity or order in which it's received. Services that use UDP are live streaming data such as VOIP, video broadcast or sensor values now. TCP is used when the data integrity and the order in

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

which it's received is important. Services that use TCP are the transfer of files in which all data and the order the data is received is important, otherwise the file will be corrupted.

- **BACnet Router:** This is a BACnet device that connects two or more networks, or two or more segments of a single network.

- **BACnet Broadcast Management Device (BBMD):** This is a specialized router for BACnet broadcast messages used to forward broadcast messages between IP subnets or to distribute broadcast messages within subnets that do not allow multicasting. For BACnet devices to operate as a system, they must be able to broadcast messages. However, standard IP technology dictates that routers do not forward broadcast messages. The BBMD resolves this problem by providing a re-broadcast on the local domain for any message originally broadcast on another domain. It is not necessary for all BACnet IP devices to support BBMD. Only one device on an IP domain needs to function as the BBMD. It will be configured to interact with BBMD's on other domains to provide the broadcast support. Additionally, a BBMD can perform a discovery of all BACnet objects reachable to a BACnet system. This functionality is primarily what distinguishes it from a BACnet router.

- **Foreign Device:** A BACnet device that has an IP subnet address different from those comprising the BACnet/IP network which the device seeks to join. The foreign device may be a full-time node on the foreign subnet or may be a part-time participant, as would be the case if the device accessed the internet via a Serial Line Internet Protocol (SLIP) or Point to Point Protocol (PPP) connection.

- **Foreign Device Registration:** For a foreign device to fully participate in the activities of a BACnet/IP network, the device must register itself with a BBMD serving one of the IP subnets comprising that network. "Full participation" implies the ability to send and receive both directed and broadcast messages. Each device that registers as a foreign device shall be placed in an entry in the BBMD's Foreign Device Table (FDT). The Register-Foreign-Device message from the client to the BBMD or BACnet router is always from one IP device to another.

2.6.3 Implementing BACnet on a Wide Area Network (WAN)

This type of implementation involves a BACnet system that has one or more BACnet objects and/or devices located on a different IP subnet than the other BACnet objects and/or devices, which are part of the same BACnet system. BACnet communicates its messages either through broadcast, which can only occur within one broadcast domain, or directed communications, which involves a message being transmitted from an IP addressable device on one broadcast across the WAN to another IP addressable device on a different broadcast domain. By making use of the GSA WAN, applications can be hosted virtually, allowing sites that share a common manufacturer to leverage the same server, as well as providing opportunities to trend and store data on a central server. Also, it is the most scalable approach that allows the creation of larger BACnet systems that may provide increased opportunities to Facilities Management related to the integration of different types of BACnet systems, such as lighting with building automation. However, projects must ensure they are effectively managing the project in such a way to avoid BACnet conflicts among different systems. Consequently, it is possible for the BACnet implementation errors from one site to negatively impact another site, perhaps even in a different region.

There are a few primary issues to consider and things to avoid when implementing BACnet on the GSA WAN:

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- All device instances associated with a BACnet network are required to be unique. ***Please Note: This can be particularly challenging on the GSA WAN, because a BACnet system implementer is likely not to be aware of the device instances of other BACnet systems that have devices, which may be discoverable over the GSA WAN.***

- Although the foreign registration process provides the ability for remote devices to participate in a particular BACnet/IP network, there may be occasions when it is desirable for two collections of BACnet/IP devices to interoperate more closely. This type of interoperation can only produce results consistent with the assumptions and intent contained in the original BACnet standard if the configuration of the two BACnet/IP networks has been coordinated.

    - If device object identifiers are not unique, the 'Who-Is' service will produce ambiguous results.

    - If multiple instances of objects with identical object identifiers exist, the 'Who-Has' service may become useless for dynamic configuration applications.

- Issues can arise when BACnet objects that are not associated with each other share a broadcast domain.

    - Most virtual servers supporting building control applications share the same IP subnet and many of those are BACnet applications. If those applications are broadcasting BACnet messages across that subnet, they can be read by any other BACnet application sharing the same UDP. Since the vast majority of BACnet systems use the default UDP, these BACnet objects are exposed to other BACnet systems. ***Please Note: Do not duplicate device instances in any single BACnet system. All regions should take inventory of their device instances and consider a regional schema and management approach to assigning device instances.***

2.6.3.1 UDP Port Assignment

BACnet systems implemented in the GSA environment shall never utilize the standard or default UDP port number designated as 47808 (BAC0) but shall be changed per regional guidance as described below. It was agreed upon by the BACnet Steering Committee that even if BACnet objects were on the same broadcast domain, they could only communicate to each other if they were using the same UDP port number. Therefore, GSA has taken a full range of possible UDP ports and assigned them to each region. Regional PBS stakeholders need to ensure they assign UDP ports that have been assigned to their respective regions. Essentially, this allows each region to take the initiative to protect itself from potential BACnet conflicts with systems in other regions. Please work with the BTSD Technical PM to access UDP port assignments for any region and/or building.

2.6.3.2 BACnet/Ethernet

Because Layer 2 network traffic cannot be effectively managed on the GSA network between subnets, BACnet/Ethernet is expressly prohibited from being implemented on the GSA WAN. BACnet/Ethernet can be used (not recommended) at a given field site, provided all BACnet devices are on the same subnet.

2.6.3.3 Using a BACnet Broadcast Management Device (BBMD)

Each IP subnet that is part of a BACnet/IP network consisting of two or more subnets shall have only one BBMD. Each BBMD shall possess a table called a Broadcast Distribution Table (BDT) which shall be the

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

same in every BBMD in each BACnet/IP network. If the BBMD has also been designated to register foreign devices, it shall also possess a Foreign Device Table (FDT).

As an example, a region may make use of BBMD devices at each field site, which enables communication of BACnet messages from their virtually hosted application servers to the BACnet objects at each field site and vice versa. In their configuration, one of the BBMDs registers the application server as a Foreign Device and keeps a table of the other BBMDs in the manufactured system's BACnet network. BACnet messages to and/or from a specific field site, or BACnet messages to and/or from the server intended for BACnet objects at specific field sites must pass through and be directed by the BBMD that has registered the server as a foreign device.

BBMDs are necessary to perform discovery of BACnet objects and can be used to affect direct communication of BACnet messages from one IP subnet to another. Only one BBMD can reside on an IP subnet on any single UDP port. This includes the subnet that hosts the virtual servers. Due to multiple BACnet applications on virtual servers that share the same subnet, a BBMD cannot be implemented on the primary virtual server VLAN. To implement a BBMD on a virtual server VLAN, two conditions must be met:

- The BBMD must be software based and able to be installed on a server that runs Windows Server 2019 (or the latest approved OS by GSA IT).

- A separate subnet must be created on the virtual server VLAN to host the BACnet system application(s) and the software based BBMD.

2.6.3.4 Foreign Device Registration

A BACnet device registered as a foreign device to a BBMD can only be referenced as a foreign device to one BBMD that is part of that BACnet system. For example, if a region has a BACnet application virtually hosted that supports multiple sites that use that application server, the server application can be registered as a Foreign Device on a BBMD at only one of the field sites. The other sites will each have one BBMD, but the Foreign Device will only be in the table of one of those BBMDs. Therefore, the BACnet messages from that server application will have to pass through the BBMD at the site that has registered the server application as a Foreign Device and then be directed to the site that BACnet message is intended for or from.

2.6.3.5 BACnet/IP Multicast

BACnet multicasting is another way to communicate BACnet messages from one subnet or broadcast domain to another. However, the GSA does not allow multicasting over its WAN. Therefore, this approach should not be considered when configuring a BACnet system on the GSA network.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Chapter 3

Cabling

3.0 Overview

This chapter will provide guidance on cable installation to support the implementation of BMC systems such as Building Automation Systems (BAS), Lighting Controls Systems (LCS), Advanced Metering Systems (AMS), Physical Access Control Systems (PACS), Photovoltaic (PV), Fire & Life Safety and Elevators. This chapter will primarily focus on guidance for Ethernet cabling, which includes Cat 5e, Cat 6/6a and Fiber Optic cabling for IP based components. ***Please Note: For questions regarding cabling for local BMC systems networks, consult with the "Building Automation Systems" chapter of the GSA Telecommunications Distribution Design Guide (TDDG).***

3.1 Cabling Roles and Responsibilities

- **GSA IT Building Technology Services Division (BTSD):** The BTSD team will work with the project managers and vendors by effectively communicating standards and providing guidance from the beginning of the design phase all the way through installation. They will also be responsible for supporting all devices on the network once cabling, switch installations/connections and device installations/connections are completed.

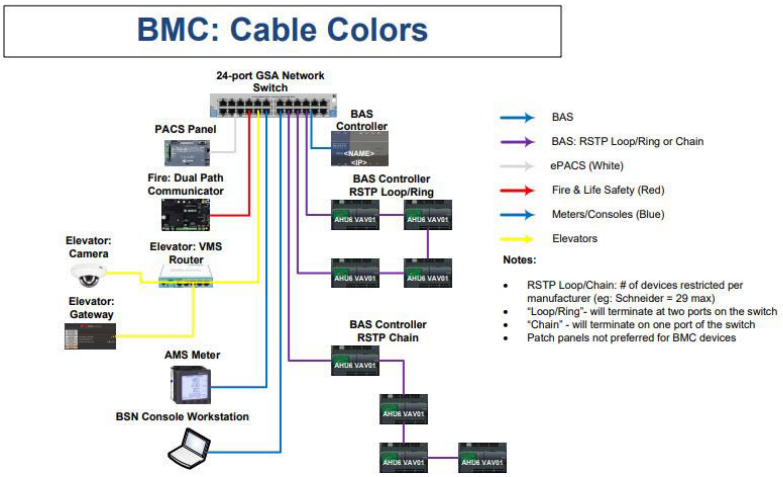
- **Regional PBS Project Teams:** This includes either facility managers and/or project managers. They are responsible for ensuring that all cabling for BMC systems contracted, purchased, owned and/or operated in the regions adhere to the *GSA Telecommunications Distribution Design Guide* (TDDG). In addition, they are responsible for contacting the BTSD prior to the award for applicable contract and implementation requirements. ***Please Note: See Chapter 4 for links to required documents.***

- **Vendors/Contractors**: The vendor/contractor is responsible for providing, installing, and labeling all network cabling. The labeling requirements are to be referenced from the *GSA Telecommunications Distribution Design Guide* (TDDG), Chapter 4, Section 4.10. ***Please Note: Regions need to take measures to ensure maintenance of the control system sub-network cables, by the vendors, are stipulated in the O&M contracts.***

3.2 Cabling Infrastructure Standards

All Ethernet cabling in the GSA buildings need to be done in accordance with the Building Industry Consulting Service International (BICSI) standards and the *GSA Telecommunications Distribution Design Guide* (TDDG). All other types of cabling installations will be handled on a case-by-case basis. All BMC systems devices require color coding the cables according to the color scheme below as well as proper labels.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514



CUI//FEDCON

Please Note: Cabling for existing BMC devices may or may not already adhere to this color scheme. Regardless, all cables must be labeled clearly and concisely to indicate what type of BSN device it is connected to.

3.2.1 Minimum Requirement for Ethernet Cabling

Please consult the *GSA Telecommunication Distribution Design Guide* (TDDG) for the latest cabling requirements as the cabling categories are rapidly changing. Depending on the scope and requirements of the cabling work, a funding source may need to be identified by the project.

- **Cabling for New Infrastructure:** For new infrastructure, the projects need to work with their controls integrator or related vendor to complete the cabling for all IP enabled devices back to the GSA provided network switches. Per the guidance mentioned in this chapter, GSA IT's approval of the GSA IP network cabling design is required.

- **Cabling Infrastructure for Existing or Migrating Systems:** To migrate an existing cabling infrastructure to a GSA approved system, cabling may need to be redesigned. In the cases, where there is not an available contract with a vendor, regions may work with their regional GSA IT manager to complete this cabling. Depending on the location of the site, and the time it will take to complete the work, arrangements for the cabling can vary, and will be handled on a case-by-case basis.

Please Note: Cat 6a is required for the device side of any wireless component installations and Cat 5e is allowed only when there is already an existing 5e infrastructure.

3.2.2 Attenuation Limit

Installing the wrong network cable can result in poor signal quality, that is why following the cabling standards is very important. The attenuation limit for Cat 5e/6 cable is 300 feet. Beyond this length, the signal quality may become unstable and transmission errors will occur. For cable runs longer than this

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

length, GSA IT will likely recommend a fiber optic run.

3.2.3 How are GSA IT Cabling Standards Enforced?

Any cabling that will provide the connection between a GSA furnished router or switch to a device that resides on the GSA Network will be required to be reviewed and approved by GSA IT. All other cabling components are to comply with Industry standards as specified in the TDDG. Any issues with cabling installed by the vendor will need to be addressed by the vendor before closing out the contract. ***Please Note: GSA IT does not assume responsibility for cabling that has not been installed in accordance with TDDG and industry standards. Please ensure the vendor is held responsible for completing the work per the TDDG.***

3.3 Cabling Installation

GSA IT encourages project managers to let vendors handle all cabling for all BMC system devices connecting to the GSA switch. This includes serial cabling, Category 5e and Category 6 ethernet cabling between the building controllers and the GSA switch. ***Please Note: Cat 6a is required for the device side of any wireless component installations and Cat 5e is allowed only when there is already an existing 5e infrastructure.***

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Chapter 4

BMC Systems Servers

4.0 Overview

This chapter will provide information on the roles and responsibilities, the BMC systems server standards, server deployment process, application installation and methods for accessing BMC systems servers.

4.1 BMC Systems Server Roles and Responsibilities

- **Technical Operations Team (TechOps):** TechOps provides guidance to the PBS organization for IT hardware, OS, database, and security compliance within the GSA standards for BMC systems, national, and regional applications for PBS systems. They are responsible for architecture design, server deployment, patching for OS and DB, providing server access when needed and troubleshooting server related issues.

- **Regional Project Teams:** The Regional Project Teams are responsible for installing the application onto the server, upgrading, and patching the application as necessary, and maintaining any other non-OS or DB components and devices.

4.2 BMC Server Standards

GSA provides virtual machines (VMs) to host building monitoring and control applications. To help meet the energy efficiency goals of GSA and move towards a virtual environment, it is standard practice for TechOps to provide VMs hosted at a GSA data center.

4.2.1 Why Go Virtual?

There are several reasons why GSA IT encourages virtualization of servers to host the BMC systems applications:

- In 2009, President Obama signed the Executive Order (EO) 3514 "to establish an integrated strategy towards sustainability in the Federal Government and to make reduction of greenhouse gas emissions (GHG) a priority for federal agencies." This executive order gives GSA and other agencies the responsibility and opportunity to find solutions to reduce energy usage and costs throughout the government.

- In 2010, Martha Johnsons' Zero Environmental Footprint Initiative (ZEF) set an agency goal for a zero environmental footprint and a 30% reduction of greenhouse gas emissions by greening the federal supply chain and creating sustainable innovation within its building portfolio. As part of ZEF, GSA IT began embracing virtualization of servers and consolidation of data centers.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- In 2012, an Office of Management and Budget (OMB) directive was issued to reduce the amount of infrastructure and promote data center consolidation (DCCI).

Please Note: GSA IT no longer provides physical servers for BMC systems. If the project stakeholders determine there is a valid need for physical hardware, procurement of the server will be the responsibility of the project stakeholders. However, they will need approval at the leadership level, and will need to coordinate hardware specifications with GSA IT to ensure compliance.

The benefits of virtualization are:

- **Reduced Downtime:** Eliminating planned downtime and preventing or reducing unplanned downtime is done through the sharing of hardware and automated restart of application servers. Properly implemented, virtualization can enable a dramatic reduction in time to recovery following a disaster.

- **High Availability:** VMware's VMotion technology enables the live migration of running virtual machines. Virtual machines do not need to be shut down for most physical server maintenance events. The VMware infrastructure will detect physical server failures and automatically restart VMs on another host. Also, TechOps has multiple access paths to the VMs compared to a single connection point with a physical server at a remote office. When a physical server at a remote office fails, server downtime is dependent on local network failures or having someone being dispatched to the site.

- **Dynamic Load Balancing:** The VMware infrastructure automatically distributes the load across a cluster of physical servers to ensure the maximum performance of all running virtual machines.

- **Hardware Flexibility:** Changing the resources available to a virtual machine is possible through a simple configuration change. Storage, processor, and memory resources can be added to meet the demand of matched to actual resource usage throughout the lifetime of the hosted application.

- **Reduced Power Consumption:** With virtualization, a single physical server can host tens of virtual machines, which reduces the power consumed per system.

- **Fast Provisioning:** Virtual machines can be provisioned quickly from a template versus installing, configuring, and shipping a physical server.

4.2.2 BMC Systems Server Hardware and Software Specifications

The GSA uses VMware software to provide a virtual environment where multiple virtual machines run in isolation, side-by-side on the same physical server host. Each virtual machine has its own virtual hardware (i.e. RAM, CPU, NIC, hard disks, etc.) and operating system to load applications. The operating system on a virtual machine does not see the hardware components of the actual physical host or any other virtual servers that utilize the physical host's resources.
As of May 2024, the BMC systems server hardware specifications are:

- Hypervisor vendor: VMware
- Memory: 8 GB
- CPU: 2 vCPUs

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- Hard Drives
  - System Drive: 100 GB
  - Application Data Drive: 100 GB

The BMC systems server software specifications are:

- Operating System: Microsoft Windows Server 2019
- Database: Microsoft SQL 2019 R2
- Web Server: IIS 10.0 (Updated as Microsoft releases)

Please Note: These specifications are subject to change. Please check with the BTSD IT PM for the latest BMC systems server build specifications.

4.2.3 BMC Systems Application Requirements

Requirements to ensure proper functionality and support on the GSA network:

- Work on VMware in a remote data center.
- Be compatible with the GSA standard hardware and software previously mentioned.
- Comply with all CIS Benchmarks for Microsoft OS and Microsoft SQL hardening.
- Allow for each cleared individual to have BMC systems software credentials.

GSA IT will <u>not</u> accept BMC systems applications that require these technologies:

- Hardware-based USB licensing (use software licensing instead)
- Applications that require Java (use HTML 5.0 instead) or any other plugins that are EOL.
- Additional embedded virtual machines
- Local computer accounts (non-Active Directory) on server for application to function.

If the application requirements are beyond the current specifications, notify the regional BTSD IT PM to avoid delays. The specifications for a new virtual server may be tailored to a specific requirement after a requirements analysis is done by TechOps. Virtual resources may also be added in the future if an application is not functioning optimally.

4.3 BMC Systems Deployment Process

The planning of BMC systems implementations that meet GSA IT standards is a collaborative effort among the TechOps, BTSD, government sponsor/project POC and BMC systems vendors.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

4.3.1 Step 1: Submit BMC Server Request Form

Prior to submitting a BMC Server Request Form, please ensure that all BMC systems software has been remediated by GSA IT Security. ***Please Note: See Section 1.4 for more details on the BMC Systems Security Assessment Process.***

Once verifying the planned BMC systems software is approved by GSA IT Security, complete a BMC Server Request Form found on PBS Systems Support Google Site. Please coordinate completing this form with the vendor and submit it to [redacted]

4.3.2 Step 2: Schedule Server Solutions Meeting with TechOps

- Schedule a meeting with TechOps by using the appointment calendar or contact TechOps by email at [redacted] to request a Server Solutions Meeting. The instructions for how to schedule an appointment are here.
- The stakeholders that should attend the Server Solutions Meeting are:
    - TechOps team member (mandatory)
    - Regional GSA POC(s) (mandatory)
    - Vendor/integrator assigned to install the application (mandatory)
    - BTSD IT PM (optional)

TechOps will review the form, plan out the architecture with the project's stakeholders and provide an estimated server delivery date.

4.3.3 Step 3: Server Deployment Process

Standard server builds are typically completed within two weeks lead time. Non-standard server builds may take longer. Once TechOps has completed the server build, they will notify all affected parties of the completion and provide the system details. All server builds include the following:

- Operating system installation and security hardening
- Database installation and security hardening
- Security and compliance measures
- Server component configuration
- Web SSL certificate generated by GSA's Internal Certificate Authority
    - SSL certificates are required to be implemented on the web interfaces of BMC systems applications hosted on GSA BMC systems servers.
    - The GSA provided SSL certificates will secure and ensure the validity of the website along with allowing these websites to be automatically trusted when accessed via web browsers of client

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

systems such as BSN consoles or the PBS Building Systems Desktop in GSA's Virtual Desktop Environment (VDI).

- The vendor assigned to install the application should have familiarity with the specific process for installing third-party SSL certificates onto the web interface for their application.

4.3.4 Do's and Don'ts for Application Installations

Do:

- Verify the installer has HSPD-12 clearance, an ENT account, and gsa.gov email account from the regional government sponsors/POCs. This is a requirement to access any GSA server.
- Use the E:\ (DATA) drive to install all software on virtual servers.
- Submit a BMC Server Monitor and Backup Request Form after installation is complete.
- Provide the BMC systems application software to TechOps to move it onto the server. This will avoid delays during the installation process.
- If full attention from a TechOps server technician will be needed during the application installation, please coordinate a date and time frame with TechOps for the requested support.
- To transfer installation files to the server, please reach out to TechOps for assistance.
- For assistance with configuring Simple Mail Transfer Protocol (SMTP)/email notifications, please reach out to TechOps.

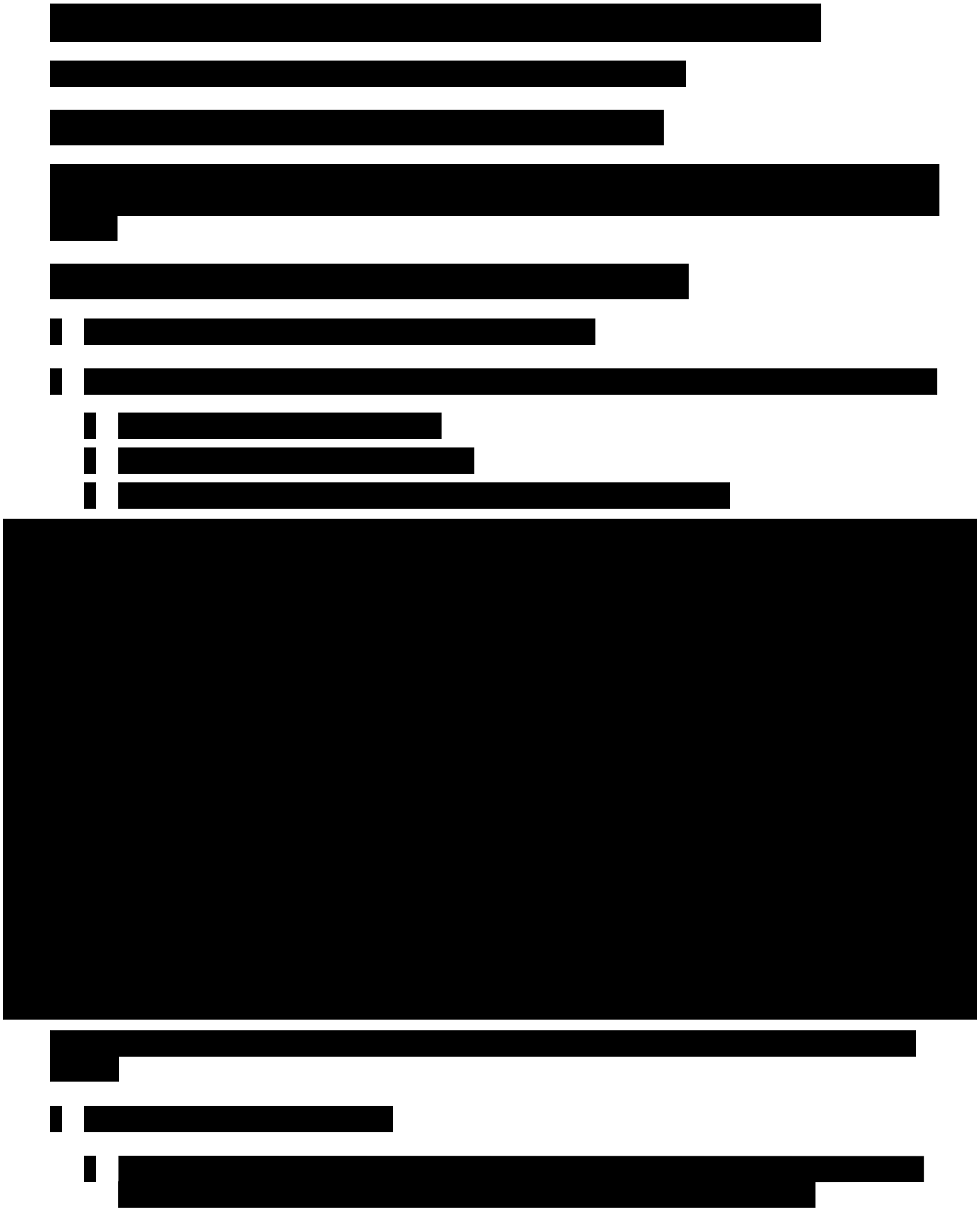
Do Not:

- Upgrade BAS software patches/minor updates without GSA IT Security Team approval.
- Use manufacturer default passwords.
- Create a local account on the server without consulting with TechOps.
- Perform any changes related to the security policies installed or configured on the system.
- Change file/folder permissions on the server without consulting with TechOps.

[redacted]

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

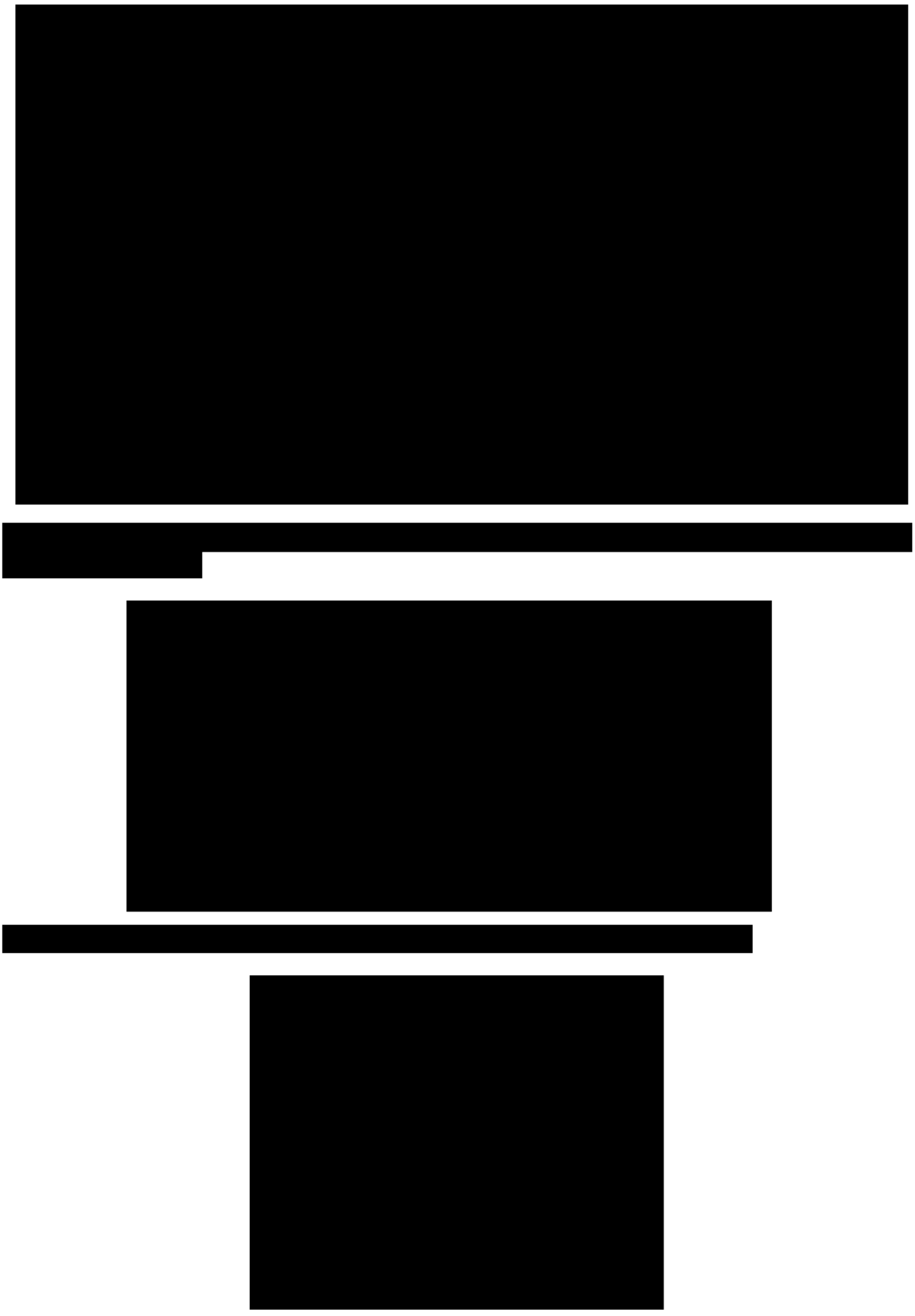


DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514



DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

[redacted]

[redacted]

[redacted]

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

4.5 Server Maintenance and Support

This section will describe server monitoring, backup solutions, patching and communications.

4.5.1 Server Monitoring and Backup

TechOps uses a software package named “Applications Manager” to monitor the health and availability of managed servers and applications. Basic server monitoring includes an availability monitor, which checks to see if the server is online through ping tests every five minutes. Advanced monitoring includes the ability to monitor services, processes, websites, and databases. TechOps is notified in the event of server health and availability failure and will take appropriate action.

Monitors will only be added if a BMC Server Monitor and Backup Request Form is submitted for the server, with the exception of server health and availability monitors. Below is a listing of the monitoring options that are offered by PB-ITS:

Windows Servers:

- Server Availability
- Disk Utilization
- Memory Usage
- Service Availability Monitoring

Websites:

- Availability Up/Down

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- Average Response Time
- Page Size
- SSL Expiration for GSA supplied SSL certificates.

Databases:

- Availability Up/Down
- Connection Times
- Log Files
- Table Space

Database Size:

- Buffer Hit Ratio
- Read, Write, Input/Output (I/O)
- SQL Statistics and Locks

Virtual servers are fully backed up. Each server's configuration, database, application, and settings are captured in one snapshot and backed up to one of GSA's data centers. Snapshots are automatically performed once a day Monday through Friday and retained locally for 30 days, which makes them readily available. After 30 days, the snapshots are kept on a tape backup for up to one year. ***Please Note: For physical servers, backups need to be discussed on a case-by-case basis with BTSD IT PM and TechOps.***

[redacted]

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

[redacted]

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Chapter 6

Technical Support for BMC Systems

6.0 Overview

There are various teams involved in supporting and troubleshooting all the different components of the BMC systems. To simplify things and get efficient help quickly, it is strongly encouraged to reach out to the regional BTSD IT PM and the SBS POC whenever there is a BMC systems related issue. Both groups can get the proper parties involved to help assist with troubleshooting efforts. This chapter outlines BMC systems maintenance and support for most of the common issues.

6.1 Technical Support Roles and Responsibilities

- **GSA IT Service Desk (ITSD):** The ITSD is the initial point of contact for all technical issues across GSA during normal business hours. They are responsible for gathering the information, creating tickets for customers, and triaging the issue to the appropriate escalation teams.

- **GSA IT Buildings Technology Services Division (BTSD):** The BTSD is the liaison between the Regional PBS Project Teams, vendors/contractors and GSA IT for all BMC systems that need to be integrated onto the GSA network. They are also one of the main points of contact for any assistance in troubleshooting the BMC systems.

- **Smart Building Specialists (SBS):** The Smart Building Specialist (SBS) POCs are the liaison between facility management, operations and maintenance (O&M) technicians and GSA IT. They are also one of the main points of contact for any assistance in troubleshooting the BMC Systems.

- **Regional Building IT Specialist (RBITS):** The RBITS primary responsibilities are to support the integration activities of building systems to the GSA network and to provide support for production systems. The individuals in this group are often located in the Regional Office Buildings (ROB) and can be sent to a site which is experiencing issues that GSA IT is unable to resolve remotely.

- **GSA IT Technical Operations Team (TechOps):** TechOps is responsible for addressing server hardware issues and server operating system issues. They are also responsible for coordinating the restoration of data backups for the applications that reside on BMC systems servers and patching the servers and consoles.

- **GSA IT Enterprise Monitoring and Event Management Team (EM&EM Team):** The EM&EM Team is responsible for troubleshooting the entire IP transport layer on the GSA IT network including all GFE routing and switching equipment. They are available for support 24/7.

- **PBS Facilities Management:** Facility manager and O&M contract staff must serve as “eyes, ears and hands” to address physical issues at the direction of the GSA IT. This may include surveying cable connections, restarting/rebooting hardware, and the installation of hardware.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- **Vendors/Contractors:** If GSA IT has determined that the issue resides with BMC systems software or hardware, the facility manager or other on-site personnel must contact the controls vendor to provide full support of the application and its proprietary hardware.

6.2 Initial Troubleshooting Steps

This is meant to be a basic troubleshooting guide for connectivity issues. If these steps do not help resolve the issue, further escalation may be needed to the appropriate team depending on the issue.

Scenario 1: Troubleshooting IP Enabled BMC Systems Hardware (Down or Unresponsive)

1) Inspect the device:

   a) Check if it is powered on/plugged in (must be always powered on).

   b) Ensure it is physically connected to the network cable.

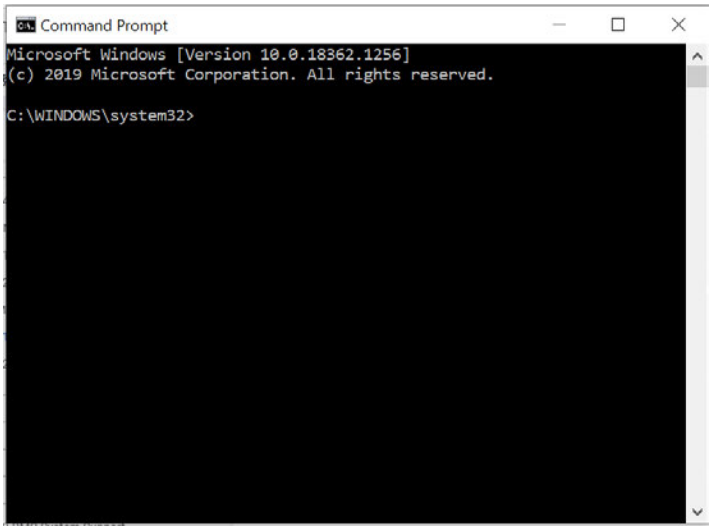
   c) Ensure the network cable is blinking at the connection (insert picture for this as an example).

2) Given that the device passed the physical inspection, attempt to ping the device from a BSN console:

   a) Log onto the BSN console.

   b) Click on the Start Menu window icon in the bottom left-hand corner.

   c) Next, type ***cmd***. Click on the command prompt to open it.



   d) Obtain IP address. If you do not have it already, please contact your BTSD Technical PM or RBITS.

   e) Type <Ping (Insert IP Address)>

      i) If the ping comes back:

         (1) If you have access rights to your application, utilize the BAS software (i.e. Niagara Workbench, Desigo, etc.) to continue troubleshooting efforts.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

(2) If you do not have access rights, please contact your sub to troubleshoot the issue.

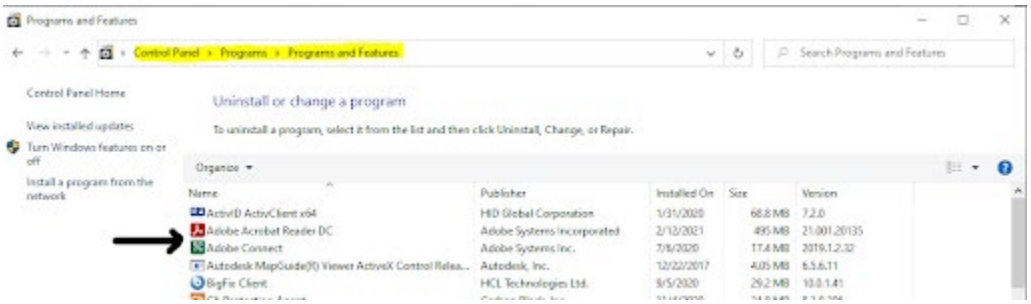
ii) if the ping fails, please contact your RBITS to further investigate the network issue. ***Please Note: Not every device is programmed to respond to a ping.***

Scenario 2: Troubleshooting BMC Systems Software

1) Please make sure that the software is installed on the BSN Console.

   a) Locate the icon on the desktop.

   b) If it's not on the desktop, go to the windows icon, control panel, program, programs and features. Confirm that it is installed.



   c) If the software is not installed, please contact your RBITS to help get the application installed.

Scenario 3: BSN Console Not Working

Please Note: The BSN Console should always be powered on and plugged into the GSA network when not being used.

1) Inspect the device:

   a) Check if it is powered on/plugged in (must be always powered on).

   b) Ensure it is physically connected to the network cable.

   c) Ensure the network cable is blinking at the connection (insert picture for this as an example).

2) Reboot the BSN console:

   a) Are there any error messages, etc.? ***Please Note: It is normal for a BSN console to display a message that there is no internet connection.***

   b) Take a screenshot of the error message and email it to (insert either RBITS and PM or distro for region or BTSD distro)

6.3 Reporting a BMC Systems Issue

Whenever a site experiences a BMC systems issue, they need to contact the appropriate personnel to assist with troubleshooting. When speaking with the support agent, be sure to first mention that the issue is related to "Building Monitoring and Control Systems." Provide the following pieces of information:

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- Building name

  Building number

  Building location (city, state, and region)

  Server, console, device name and/or IP address, if applicable

  BMC system or software name, if applicable

  MAC address, if applicable

  Network connectivity issues, if applicable

  Application or device accessibility from BSN Console, Citrix VDI or Remote Desktop Protocol, if applicable

  Last known date or time the system was working/ approximate date or time when the issue started.

  Any recent changes made in the environment that could have caused the problem.

  Provide screenshots, if possible

For normal business hours, the site POC must go through the regular channels to create an Incident ticket.

- Call the GSA IT Service Desk hotline at 866-450-5250. Their normal business hours are Monday - Friday, 7am - 8 pm Eastern Standard Time.
- Select option 5 “Application Support”.
- Then, select option 2 “Building Monitoring and Control Systems”.
- Once the ticket is created, please send an email to the regional BTSD IT PM and SBS POCs with the ticket number as well as any other pertinent information and they will contact the appropriate groups as needed.

Please Note: GSA IT has limited support options after hours. The main two types of options are support for servers at the OS level and any network connectivity issues.

For any server related emergency requests after hours:

- Email TechOps at [redacted] and copy the regional BTSD Technical PM and SBS POCs. For any emergency requests, they will typically respond within an hour. Any non-emergency requests will be addressed the next business day.
- If there is planned maintenance on a system outside of normal business hours that requires support from TechOps, please coordinate this prior to the scheduled maintenance.

For any network related issues after hours:

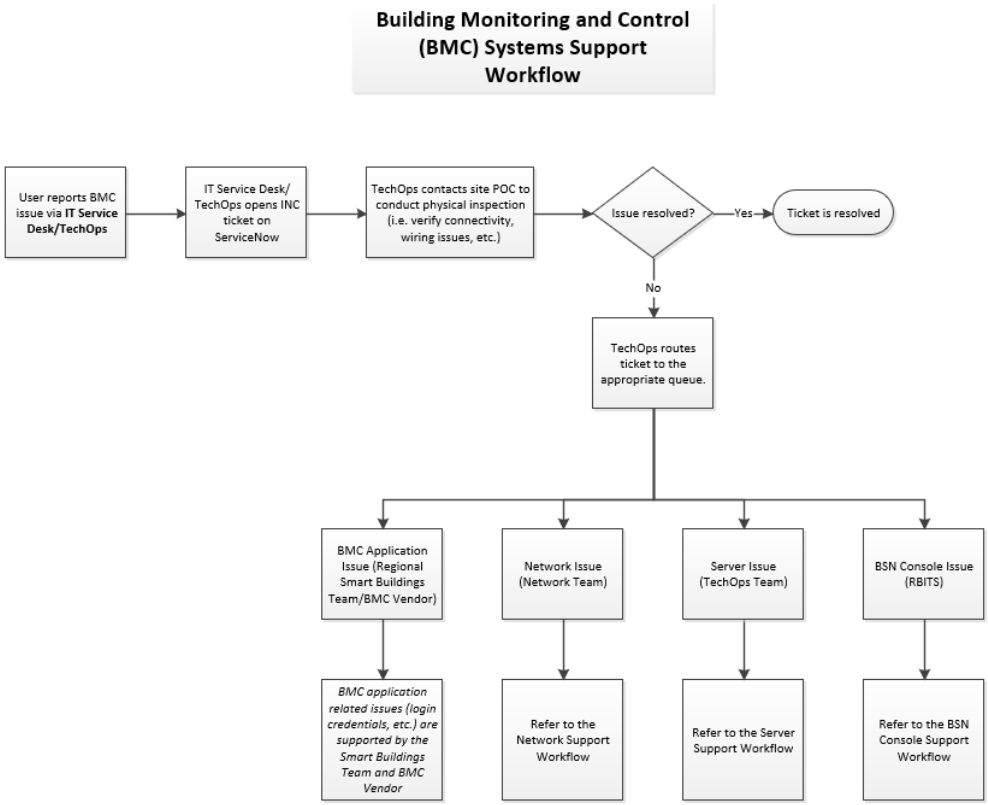
- Call EM&EM at [redacted]

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- Select option 2 to report a critical enterprise-wide outage or service disruption. This option will escalate you to a person who can assist immediately.
- Once the ticket is created, please send an email to your BTSD IT PM and SBS POC(s) with the Incident ticket number as well as any other pertinent information. If the ticket is still not resolved after hours, they will escalate to the appropriate groups the next business day.

6.4 BMC Systems Support Workflow

Below is an example of a typical troubleshooting workflow. The IT Service Desk opens an incident ticket, which they route to other queues depending on the suspected issue. The four main categories that issues typically fall under are BMC systems applications, BMC systems hardware, network, server, or BSN console.



6.4.1 BMC Systems Application Issue

If the BTSD IT PM or Smart Buildings Specialist (SBS) PM suspects it's a BMC systems application issue, the SBS PM will reach out to the appropriate vendor support contract personnel to troubleshoot issues such as login credentials, etc.

6.4.2 BMC Systems Hardware

If the BTSD IT PM or Smart Buildings Specialist (SBS) PM suspects it's a BMC systems hardware issue, they will help the site POC get pricing for the replacement of the hardware, put together the contract necessary to replace the device and schedule the work.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

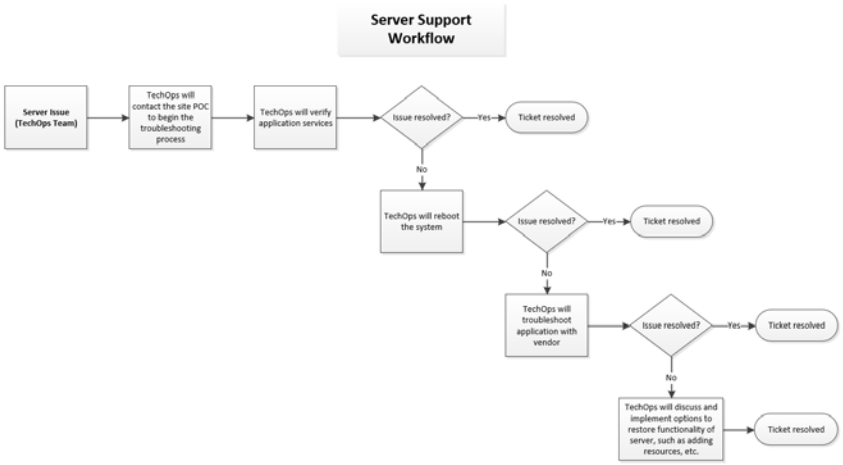
6.4.3 Network Issue

If the BTSD IT PM or Smart Buildings Specialist (SBS) PM suspects that the issue is related to a router, switch, etc. they will typically route the ticket to the EM&EM (formerly known as the NOC). Below is the workflow demonstrating the troubleshooting steps the EM&EM team takes when trying to resolve a network issue. The contact information for the EM & EM team is [redacted] They support the buildings 24/7 for major network outages or incidents.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

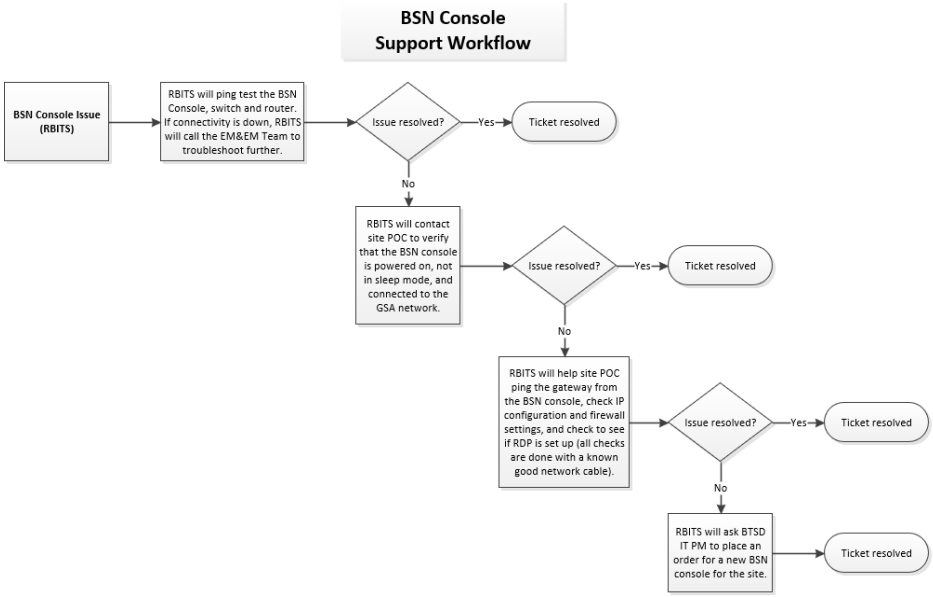
6.4.4 BMC Server Issue

If the BTSD IT PM or Smart Buildings Specialist (SBS) PM suspects that the issue is related to a BMC systems server, they will reach out to TechOps to help troubleshoot the issue. Below is the workflow demonstrating the troubleshooting steps the PBS System Support Team takes when trying to resolve a server issue. The contact information for TechOps is [redacted] and their normal business hours are Monday through Friday 7am - 7pm Eastern Standard Time. They can be reached after hours from 7pm - 7am Eastern Standard Time for emergency related requests only.



6.4.5 BSN Console Issue

If the BTSD IT PM or Smart Buildings Specialist (SBS) PM suspects that the issue is related to a BSN console, they will reach out to the RBITS to help troubleshoot the issue. Below is the workflow demonstrating the troubleshooting steps the RBITS Team takes when trying to resolve a BSN console issue. The contact information for RBITS is [redacted] and their normal business hours are Monday through Friday 8am - 5pm Eastern Standard Time.



DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Chapter 7

Advanced Metering System (AMS)

7.0 Overview

The advanced metering program is a multi-tiered, Commercial-off-the-Shelf (COTS) solution designed to monitor and store energy consumption that includes 11 production servers. It collects meter data on electricity, gas, steam, hot water, domestic water, photovoltaic and limited sub-metering. GSA has an inventory of approximately 40 unique devices with over 700 IP enabled devices, and 1900 serial meters, across approximately 500 facilities.

The platform consists of one enterprise cloud server, currently hosting Envizi (MUSE) application, and 11 dedicated regional metering servers (R1-R11), hosting the Schneider Power Monitoring Expert (PME) application. The 11 servers are managed centrally, as part of the Advanced Metering Systems (AMS) program by GSA IT. The Schneider PME application is supported by a team of consultants from Schneider Electric. The metering hardware is maintained by an O&M group, Redhorse, who is responsible for resolving metering issues.

7.1 Advanced Metering System Roles and Responsibilities

- **IT Project Manager for Advanced Metering Systems:** The AMS IT project manager works closely with the PBS program office, coordinates upgrades and releases with TechOps and works closely with ISSO to ensure the application is compliant with security requirements.

- **PBS Program Manager Advanced Metering Systems:** The program manager conducts a daily review of Source Activity and trend summaries to identify any data issues at a regional or national level. They also conduct bi-weekly project calls with Schneider Electric to discuss all integration efforts, application issues, upcoming projects, security scans and issues, training needs and software issues and conduct weekly project calls with Redhorse regarding all aspects of metering support. They also monitor Uplight (virtual auditing program) reports to trends to ensure that buildings with evaluation requirements have the data needed for evaluations. Additionally, they coordinate training webinars for end-users and conduct quarterly metering network calls with the national and regional AMS community.

- **Program Lead:** The program lead is responsible for providing end users with dashboards and training necessary to effectively interpret metering data (facility managers, O&M contractors, etc.). They are responsible for maintaining the metering infrastructure and installation. Program leads use the data as a tool for finding opportunities for energy savings. They also use the data to evaluate building performance for design development and use data post-construction to evaluate building performance.

- **Regional Lead:** The regional lead documents and manages the inventory of regional advanced meters. Project manages the initial installations, integrations, and replacements of regional advanced meters according to the priorities set forth by the PBS Program Manager Advanced Metering System and Facility Management. The regional lead works closely with a team of engineers to serve as the liaisons

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

between the facility managers and the advanced metering contractors (Red Horse and Schneider Electric). The regional lead is also the front facing role for all advanced meters inquiries initiated by regional management and building managers.

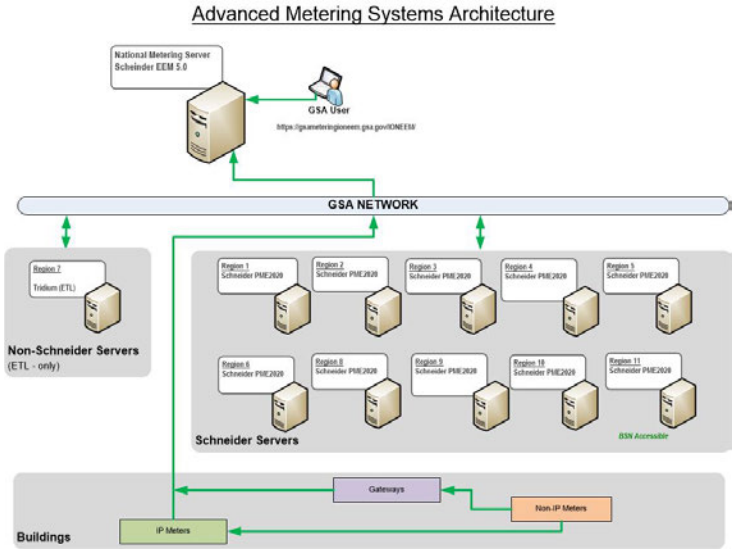
- **Schneider Electric:** Schneider Electric has a dedicated team of technical support consultants that are responsible for the PME application. They provide metering support from the application to the end-user, which includes metering integration, updating network diagrams, source management, ensuring the system is functioning and reporting on system health.

- **Redhorse:** Redhorse is a contracting support service company that logs and manages all the tickets related to the Advanced Metering program and produces the weekly Source Activity Report that provides a count of all advanced meters that are down across GSA. They are also responsible for the repair and replacement of meters and other hardware components like gateways, transponders, converters, and wiring. Along with Schneider Electric, they provide the information necessary for Schneider Electric to update AMS network diagrams.

- **Facility Managers/O&M Contractors:** Facility Managers/O&M contractors are responsible for confirming meter communication status at their locations and looking at metering data on a regular basis. The O&M partners with GSA to fully utilize the AMS to develop and implement strategies that will result in an overall reduction in energy consumption. The O&M must verify daily that each of the advanced meter(s) are functioning properly and are communicating to the regional and Central Office server, as applicable, and are accessible via end-user interface. The O&M are also responsible for correcting any onsite communication failure immediately to mitigate any loss of data.

7.2 Advanced Metering System Architecture

The AMS Architecture includes approximately 40 unique devices with over 700 IP enabled devices, and 1900 serial meters, across approximately 500 facilities. Most of the devices report 15-minute interval data directly to the corresponding regional PME server. Subsequently the data is moved to the national metering server (MUSE) to provide users with dashboards, reports, and trends.



DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

7.3 Standards for Interoperability

The following is a high-level list of items to consider for the implementation of any new meters.

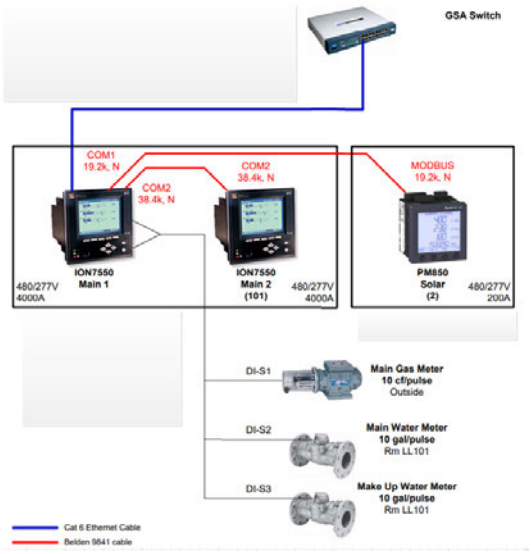
- Prior to deployment, all IP enabled meters will be subject to scanning and certification. ***Please Note: See Section 1.4 for details on the BMC Systems Security Assessment Process.***
- All IP ranges/addresses are provided by GSA IT Network Team, in coordination with the BTSD IT PMs.
- The MAC address for all IP meters must be whitelisted before they are allowed to connect to the GSA network. ***Please Note: See Section 1.2.4 for the process of whitelisting devices.***
- All devices must be IPv6 capable to be installed on the network.
- All IP meters on the GSA network are subject to continuous monitoring and periodic scanning by GSA IT.

7.4 New Installations

This section will discuss the requirements for the network diagram as well as cabling installation.

7.4.1 Sample Network Diagram

Network diagrams (see simplified sample below) help the AMS support team or GSA IT expedite resolution of issues. In the example below, the site has one IP enabled ION 7650 electrical meter, and a gateway that is connected directly to the switch. Downstream of that meter/gateway is a serially connected ION 7650, a Solar meter connected serially via Modbus, and 3 serially connected water meters.



Please Note: This diagram is different from a network diagram. See Section 2.3.2 for a sample network riser diagram that needs to be submitted to the BTSD IT PM for all new metering integrations.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

7.4.2 Cabling

GSA IT requires facility managers to coordinate cabling with a local vendor for completing all runs back to the GSA-provided switches and shall be installed in collaboration and in accordance with the *GSA Telecommunications Distribution Design Guide* (TDDG). ***Please Note: Troubleshooting cabling issues is not the responsibility of GSA IT and will need to be coordinated with the cabling vendor.***

7.5 Technical Support for AMS

Redhorse is responsible for supporting the meters at GSA on a national level. They monitor PME and MUSE on a regular basis to see what IP enabled meters are offline. Typically, Redhorse is proactive about troubleshooting offline meters with GSA IT and Schneider and will reach out to the site for assistance as needed. Additionally, some regions have a contract with the O&M staff to recalibrate, repair or troubleshoot the AMS. If this is the case, then they can perform their initial troubleshooting steps and then contact Redhorse when further escalation is required.

7.5.1 Support Form

If the site experiencing issues does not have an O&M support contract in place for meters or needs further troubleshooting assistance from Redhorse, they can fill out the Advanced Metering: Support Request Form. This form provides Redhorse the information necessary for troubleshooting most issues. The following information must be collected by the regional POC/O&M tech to submit the form:

- Is this a new or existing problem?
- Region
- Type of Problem:
    - Communications or data loss with meter(s) at a specific building.
    - Data is reporting, but it is incorrect for a specific building.
    - ION EEM or PME server problems (e.g. problems with trends, subscriptions, modules, or other functionality)
    - I want nodes or meters deleted from the system.
- Building ID Code (i.e. AA0000ZZ)
- Point of Contacts:
    - Regional Point of Contact
    - Onsite Point of Contact (Property Manager, O&M Contractor, Facility Operations Specialists) ***Please Note: This is important, the submitter needs to give someone who Redhorse can work with to troubleshoot.***
    - Any Additional Point of Contacts

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- Offline Meter Type
  - ALL meters are not reporting.
  - Electric Main
  - Electric Sub Meter
  - Gas
  - Steam
  - Chilled Water
  - Water
  - Renewable energy (e.g. PV inverter)
- Meter Description: Utility, Manufacturer, Series, & Models
- Total Number of Devices Affected
- Building Switch Name (Upstream of Meter)
- Building Switch IP Address
- Building Switch Port
- Main Meter IP Address
- MAC Address
- Have you pinged the meter?
- A Network Diagram
- A Switch Matrix Spreadsheet
- Any pictures of the meters, cables, switches, or other equipment that can help diagnose the problem.
- Additional comments or notes about the meters at this location including previous steps taken or known events at the building that could have caused the problem.

For assistance with filling out the support form, please contact:

[redacted]

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

7.5.2 Troubleshooting Process

- Redhorse will generate an Incident Ticket in ServiceNow based on the responses from the Support Request Form.
- Based on the responses in the Support Request Form, Redhorse can generally determine what type of issue it is: application, network, or hardware.
- For application issues, Redhorse will contact the AMS IT PM. The AMS IT PM would then determine if the issue resides in MUSE or PME.
    - If the issue resides in MUSE, the AMS IT PM would contact IBM to troubleshoot the issue.
    - If the issue resides in PME, then the AMS IT PM would contact Schneider Electric to troubleshoot the issue.
    - If the data in PME passes through the GSA Secure File Transfer Services (SFTS) server, the AMS IT PM would contact the GSA SFTS server team to troubleshoot the issue.
- For network issues, Redhorse does initial troubleshooting steps (i.e. pinging devices, etc.) After a failed ping, Redhorse may arrange a physical inspection of the device with the help of the Regional POC/O&M Tech. They may ask to power cycle the switch. If that does not help with the connectivity issue, they would call EM&EM to further troubleshoot the network connectivity.
- For hardware issues, Redhorse may ask the O&M tech onsite to power cycle the metering device. If the device still does not work properly, Redhorse will have to repair or replace the device. Redhorse would have to then contract a local vendor or integrator (i.e. American Systems) to do a site survey and give an estimate for the work. Redhorse then would purchase the meter and provide a purchase order to the experienced technician (i.e. Schneider) to get the meter replaced and integrated.
- Redhorse will resolve the incident ticket when an agreeable solution is provided for the issue.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Chapter 8

Physical Access Control System (PACS)

8.0 Overview

This chapter will provide guidance on access management tools being utilized for GSA-controlled space leveraging the GSA IT infrastructure. A system composed of hardware and software components that control authenticated access to physical facilities by granting/denying access based upon results from electronic validation and authentication. Physical Access Control System (PACS) is a form of access management tools consistent with governing policies. PACS is a physical access control system that utilizes contact/contactless smart-card recognition, access codes, biometrics, or a combination thereof to gain entrance into secured areas.

All GSA related PACS projects and/or GSA controlled space within the GSA inventory must be fully compliant with *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors*, *FIPS 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors*, and *OMB Memorandum 19-17*, which sets the Federal Identity, Credential and Access Management (ICAM) standards. Therefore, all GSA PACS projects will adhere to *GSA Order ADM 5900.1* as the guiding document for the agency's national strategy related to PACS requirements.

Most compromises to the GSA network originate from within GSA (ENT) networks because of users downloading malware via spam or from a compromised site. The malware seeks to burrow deeper into systems via this "pivot point." This aspect, in combination with the inherently sensitive nature of information (PII), potentially accessible via PACS, requires a more robust approach to security than currently required with other BMC systems. To this effect, a dedicated chapter was developed for these systems.

8.1 Physical Access Control Systems Roles and Responsibilities

- **GSA IT Deskside Services:** The Deskside Services Team (formally known as "local support") model for these types of systems will be the same as other BMC systems projects. GSA IT will provide, image, and support GSA PACS Enrollment and Guard-Viewing Stations, like any other ENT machine. GSA IT will be responsible from the remote end of the Ethernet cabling termination back to and through the GSA network and will ensure network transport of IP traffic. The region/site is responsible to secure any additional funding or support that exceeds what the National PBS contract provides at a basic level.

- **GSA IT Technical Operations Team (TechOps):** TechOps will support any virtual server supplied by TechOps for any initiative related to a PACS deployment per their normal Standard Operating Procedures (SOP) and support guidelines.

- **GSA IT Building Technologies Service Division (BTSD):** The BTSD team's roles and responsibilities related to PACS will be like other BMC Systems. The BTSD will work in conjunction with The Office of Mission Assurance (OMA), GSA IT and PBS. The BTSD will assist with the network infrastructure, authorize, and issue IP addresses, submit MAC whitelisting requests (after provided by OMA), and

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

perform basic troubleshooting for connectivity issues the integrator may experience, or if needed, coordinate with the network team for larger scale complications. PBS will act as the primary Project Manager for all PACS projects, while OMA will continue to maintain oversight, provide SOPs for on-boarding, migration strategies, methods of compliance, and requirements.

- **GSA IT Network Operations Division (Network Team):** The Network Team is responsible for providing network connectivity for the entire IP transport layer to PACS. They shall provide installation, network management and monitoring, and security and reporting services for PACS. The support services include management and monitoring of IP network switches, routers, and physical network connections to PACS. They are responsible for producing and analyzing network statistics for the various components of the network to determine and implement adjustments and improvements for optimized network performance. Lastly, the Network Team provides high level troubleshooting, fault isolation, and correction support for the PACS networks. They shall perform the following services:

    - Provide design, configuration, installation, and documentation services for PACS network.

    - Coordinate configuration, testing, adjustment, and implementation of PACS connections.

    - Participate in the installation, de-installation, and interconnection of PACS LAN equipment as well as interconnection between WAN equipment and circuit interfaces.

    - Participate in the installation, de-installation, and interconnection of PACS to the LAN interfaces.

    - Segment PACS on Virtual Local Area Networks (VLANs), VLANs 55 and 504/505 respectively, and subnets.

    - Establish access control list (ACL). Only authorized systems will be allowed access to PACS systems.

Please Note: As previously identified, the differences between Building Monitoring and Control Systems and the need for an elevated security posture for the PACS systems that comply with the National Scope of Work dictate that they must NOT reside on the BSN and will not be able to communicate directly with any system/device(s) that are on the BSN.

- **Public Building Service (PBS):** PBS is responsible for providing a project manager, facility or building manager, and contracting officer for any PACS projects. PBS will work with OMA to ensure all PACS projects comply with ADM 5900.1 and align with the OMA National PACS Framework. PBS will coordinate all aspects of facility management and work with OMA and GSA IT to ensure all agency requirements are met with regards to PACS installations and maintenance, including basic site troubleshooting.

- **Office of Mission Assurance (OMA):** OMA is responsible for issuance and maintenance of all agency internal documents related to the implementation of a national (enterprise wide) EPACS solution. OMA ensures all GSA related PACS projects and/or space within the GSA inventory is compliant with *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors*, *FIPS 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors*, and *OMB Memorandum 19-17*, which sets the Federal Identity, Credential and Access Management (ICAM) standards. OMA ensures GSA projects for GSA controlled space follows the *National EPACS Scope of Work (SOW) for PACS Integration Migration* and adheres to *GSA Order*

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

ADM 5900.1 as the guiding document for the agency's national strategy related to PACS requirements. It will be the responsibility of OMA (with the support of GSA IT and PBS) to ensure PACS compliance with all related and referenced policy documents. OMA will provide guidance on the procurement, implementation, administration, and oversight for physical security countermeasures (aka "fixtures") as outlined in the *Memorandum of Understanding (MOU) Addenda 002 Between General Services Administration (GSA) and Department of Homeland Security (DHS)*. Regarding O&M of PACS, OMA will manage National PACS O&M and Licensing contracts to provide minimal support for PACS components, a pathway to a certified installer/technician, and licensing to avoid lapses in SSAs and licensing requirements. For any hardware or system related PACS issues, OMA will work with PBS and GSA IT to triage and troubleshoot or escalate to the PACS O&M contractor to resolve. OMA will work with GSA IT and PBS to continually assess and determine the best and most cost-effective approach for support. OMA will work to ensure policy or mandate changes are communicated to all stakeholders accordingly to facilitate compliance.

8.2 Security

All PACS devices that are, will be or are being considered for use on the GSA network not only must comply with the OMA National PACS Framework but must also be evaluated and remediated in accordance with BMC IT Security procedures. The evaluation process will consist of security scans, a manual evaluation, and the creation of a Security Assessment Report (SAR). The assessment process is detailed in *BMC Systems Security Assessment Process [CIO IT Security 16-76 Rev 4]*. ***Please Note: For more information on the BMC Systems Security Assessment Process, please see Section 1.4.***

Specific Security Requirements for GSA PACS Systems:

- All PACS devices that will be implemented on the GSA network must adhere to current GSA IT security policies.
- All critical and high vulnerabilities identified must be mitigated within 30 days and all moderate vulnerabilities mitigated within 90 days or require an Acceptance of Risk to be signed by the Authorizing Official (AO).
- All hardware must be hardened according to GSA hardening guides or CIS Level 1 benchmarks.
- All system users must have appropriate HSPD-12 background investigations completed.
- Systems must have on-going support to achieve or maintain an Authority to Operate and remain in compliance with GSA Security policies.

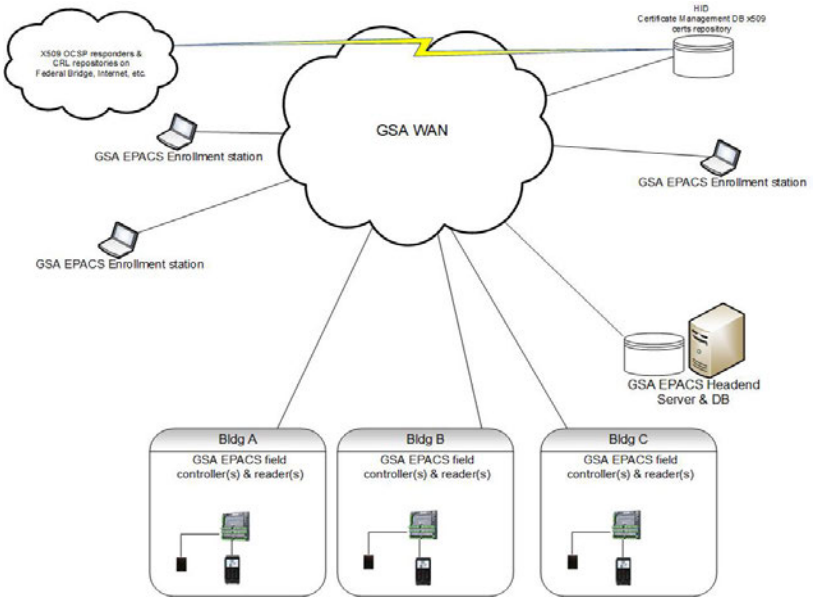
8.3 PACS Architecture and Integration

The PACS network architecture consists of a centralized headend and centralized certificate management server that each Field Office Building (FOB) connects to and is integrated with. All PACS projects and integrations must meet current GSA, GSA IT, OMA policies, and other applicable Federal guidance, directives, policies, and mandates. Each PACS project must communicate and coordinate with the OMA Physical Access Control Systems Branch to ensure the PACS project meets the standards set-forth by OMA, GSA and other applicable Federal guidance, directives, policies, and mandates. It is required that the vendors selected to do the PACS implementation and integration be certified installers for the field

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

devices as well as the centralized headend and certificate management devices. ***Please Note: Head-end refers to a server-based system that pushes settings down to the respective readers/panels.***

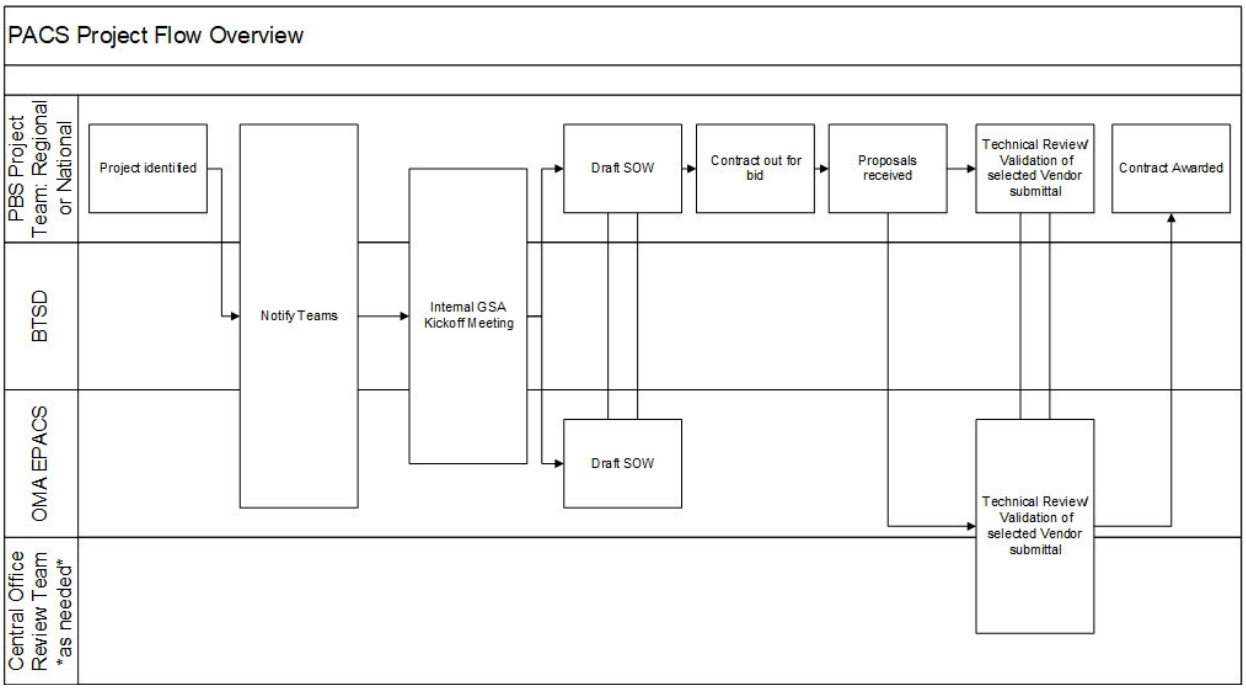
The following diagram provides the layout for the regional network architect:

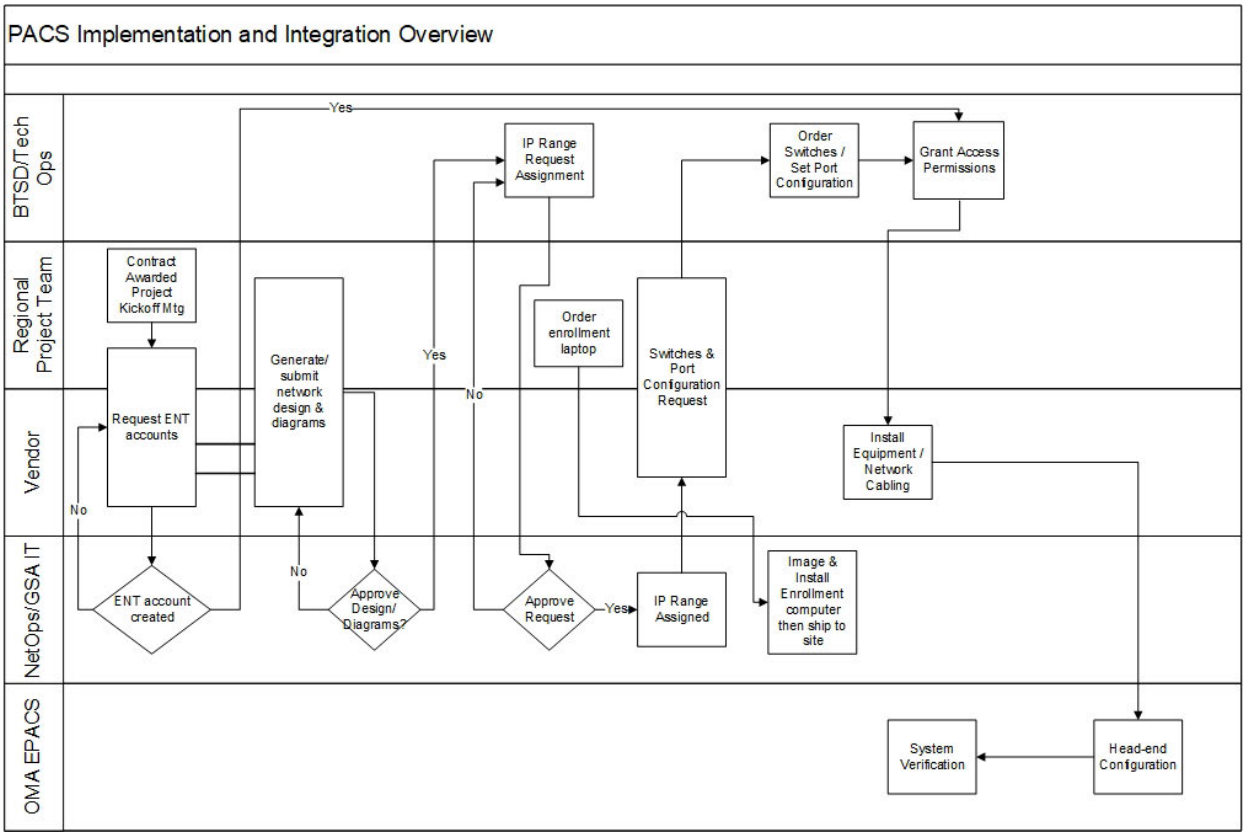


8.4 Project Flow

The following are basic process flows for PACS projects from identification through installation and integration. ***Please Note: The Central Office Review Team consists of TechOps, Network Team and Security Team. The following process diagrams are providing a high-level overview only & are not to be used to represent every step in either process.***

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514





DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

8.5 GSA IT EPACS Support

All EPACS system and hardware troubleshooting and triage starts at the EPACS level. In the instance a user needs assistance, please contact [redacted] ***Please Note: Any user or card-related issues do not fall under this type of elevated support.***

All user and card-related issues are managed at the facility level and are sent to [redacted] During triage of any PACS issues related to hardware connected to the GSA network, any necessary involvement with Network Services or GSA IT needing IT tickets for these systems will follow the same flow as for all other BMC systems. TechOps and/or the Network Team will triage the tickets as they currently do for BMC systems related issues. ***Please Note: See Section 5.4 for details on how to report a BMC systems issue.***

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Chapter 9

BMC Systems Procurement: Contract Language & IT Requirements in Scope of Work

9.0 Overview

This chapter entails recommended 'scope of work' and contract language requirements for building systems procurements. This document also includes pertinent IT security policy references. Please work with the Contracting Officer to incorporate these requirements into the proper sections of the building controls solicitation. ***Please Note: PBS regions may have further defined requirements, or standards may exist that would otherwise add to and/or specify use of regional standardized systems. In those cases, vendors must adhere to those requirements. If there are no specific regional standards in place, then requirements will default to PBS' national standards (i.e. the Building Automation System (BAS) BPA).***

9.1 Contract Language IT Security Requirements

1.0 IT Security Requirements

Vendors of [X Project] are required to meet the GSA IT Security and Privacy requirements identified in the ensuing sections.

2.0 IT Security Assessment and Authorization Requirements

Contractors must obtain an Authorization to Operate (ATO) for the proposed solution at the FIPS 199 Moderate impact level. Service Providers offering solutions delivered as-a-service in the cloud, meeting the *NIST SP 800-145: The NIST Definition of Cloud Computing*, consistent with the OMB FedRAMP Policy memo, are subject to FedRAMP cloud information security and privacy requirements. Vendors with traditional on-premise or cloud deployments (not delivered as SaaS) are required to meet traditional GSA Assessment and Authorization (A&A) requirements. Vendors having mobile application components are required to meet the additional mobile application security requirements as defined in Section 9.2.5. Further, any software required for installation on Government Furnished Equipment (GFE), or hardware required for deployment in GSA Facilities is subject to GSA software and device testing processes as defined in section 9.2.4.

3.0 Cloud Delivered as-a-Service (Requires FedRAMP)

Cloud computing offers an opportunity for the Federal Government to take advantage of cutting-edge information technologies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services provided to its agencies and citizens. Established by OMB in 2011, The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP empowers agencies to use modern cloud technologies, with emphasis on security and protection of federal information. Federal executive departments and agencies procuring commercial and non-commercial cloud services that are provided by information systems that support the operations and assets of the departments and agencies are required to ensure applicable contracts appropriately require cloud service providers (CSPs) to comply with FedRAMP security authorization requirements. This includes systems across all cloud deployment models (e.g., Public Clouds, Community Clouds, Private Clouds); Hybrid Clouds) and all cloud service models (e.g., Infrastructure as a Service, Platform as a Service, Software as a Service) as defined per *NIST SP 800-145: The NIST Definition of Cloud Computing*.

The Cloud Information Systems – IT Security and Privacy Requirements identified in Chapter 5 of the *Security and Privacy Requirements for IT Acquisition Efforts [CIO-IT Security 09-48, Rev. 7]*, Security Language for IT Acquisition Efforts is applicable at the FIPS 199 Moderate impact level. Personally Identifiable Information (PII) is ***not*** in the scope of acquisition and PII is not expected to be stored in the service provider's cloud solution.

Vendors are required to submit and receive GSA's approval of documentation as evidence of complying with the security requirements listed in Chapter 5 prior to being able to accept any orders.
Changes to the platform that impact the security authorization throughout the period of performance will require attendant changes to maintain the security authorization.

Vendors are required to either be already FedRAMP authorized or be able to achieve a FedRAMP Moderate authorization within One (1) year of the contract award. If not already FedRAMP authorized at the FIPS 199 Moderate impact level, GSA can work with the vendor to obtain a GSA MiSaaS (Moderate Impact Software as a Service) Authority to Operate (ATO) from GSA IT Security within 150 days of the notice to proceed. Onboard base year projects within 30 days of obtaining MiSaaS ATO. **No Government data can be uploaded into the production software application until the GSA Authority to Operate (ATO) is obtained**.

Vendors pursuing awards under this solicitation are required to partner with a Third-Party Assessment Organization (3PAO) to facilitate an independent assessment of the offeror's documented and implemented NIST 800-53 security controls. Vendors are encouraged to also attain 3PAO services for documentation preparation.

Vendor shall adhere to a milestone schedule to ensure compliance with first year FedRAMP requirement. If at any time, the vendor is either unwilling or unable to meet any of the process requirements, GSA may choose to terminate the award.

4.0 Traditional On-Premise or Cloud Delivered (not SaaS)

- **4.1 External Hosted or Cloud Delivered**

  Vendors choosing to offer a solution hosted on their system should reference The External Information Systems – IT Security and Privacy Requirements identified in Chapter 2 of the *Security and Privacy Requirements for IT Acquisition Efforts [CIO-IT Security 09-48, Rev. 7]*. Security Language for IT Acquisition Efforts is applicable at the FIPS 199 Moderate impact level. The vendor shall be required to obtain a GSA IT-Security Authority to Operate (ATO). For further guidance on ATO, reference *Managing Enterprise Cybersecurity Risk [CIO-IT Security 06-30 Rev-24]*.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- **4.2 On-Premise (GSA) Hosted**
  - Vendors choosing to offer a solution hosted within GSA environment should reference the Internal Information Systems - IT Security and Privacy Requirements identified in Chapter 3 of the *Security and Privacy Requirements for IT Acquisition Efforts [CIO-IT Security 09-48, Rev. 7]* is applicable at the FIPS 199 Moderate impact level. The vendor shall be required to obtain a GSA IT-Security Authority to Operate (ATO). For further guidance on ATO, reference *Managing Enterprise Cybersecurity Risk [CIO-IT Security 06-30 Rev-24]*.
  - Additionally for any smart buildings or IoT components, the vendor should adhere to the Building Technologies Technical Reference Guide version 3.0 (or the latest posted version).

Vendors pursuing awards under this solicitation are required to partner with an independent assessor (GSA is required to approve) to facilitate an independent assessment of the offeror's documented and implemented *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations* security controls. Vendors are encouraged to leverage a 3PAO for assessment services and for documentation preparation.

5.0 Hardware Device and Software Security Testing for Components Required for Deployment in GSA Facilities/Networks (If any)

Per *BMC Systems Security Assessment Process [CIO IT Security 16-76 Rev 4]*, all IP addressable devices, appliances and software applications that will communicate over the GSA network shall be reviewed by GSA IT. Before any hardware, software or IT/IoT device/system is connected to its network, a security risk assessment of selected management, operational, and technical security controls is performed, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. A security assessment report is produced by GSA IT, which will be provided to the PBS stakeholders and the vendor. The assessment report will allow GSA to understand and accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. The contractor/vendor shall therefore be held responsible for mitigating all security risks identified.

Vulnerabilities shall be mitigated, within the following timeframes:

Severity	
Critical and high vulnerabilities	≤ 30 business days
Moderate vulnerabilities	≤ 90 business days

The GSA IT Security Team performs security control reviews utilizing a systematic, repeatable approach, which is utilized to uniformly evaluate any device, application, or general support system.

Once the device/application has completely gone through the remediation process and has a remediation/hardening plan in place, all other projects can use that report to configure the named device,

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

or application accordingly. This assessment is revisited every three years, or upon release of any major new revision of the solution, at any stage when new vulnerabilities are uncovered and reported (i.e. ICS-CERT advisories). The contractor(s) will therefore need to have a strategy to address evolving vulnerabilities in timelines set by GSA.

- **5.1** Per White House *Office of Management and Budget (OMB) Memorandum 21-07 (M-21-07)*, the Federal Government will deliver information services, operate networks, and access services of others using only IPv6. Starting no later than FY23, all new networked federal BMC systems must be IPv6 enabled when deployed. The intent is to phase out IPV4 for all federal BMC systems. Currently, our network and client devices are IPv6-enabled, but the applications and the systems they run on, including servers and databases are likely not capable based on their current configuration. GSA must accept only IPv6 enabled systems when deploying new networked federal BMC systems. The intent is to phase out all IPv4 systems over the next several years. IPv4 will no longer be allowed for new projects/assessments starting July 2023. Break/Fix replacements of existing (deployed) hardware should prioritize utilizing an IPv6 capable replacement when possible.

- **5.2** Per the *Internet of Things Cybersecurity Improvement Act of 2020* and the White House *Office of Management and Budget (OMB) Memorandum M-24-04*, the Federal Government will only purchase Internet of Things devices that comply with *NIST SP 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*. As defined in the guide, any devices provided by the contractor that meet the definition of IoT, must meet the guide's security requirements.

6.0 Mobile Application Security Requirements (If Applicable)

The contractor shall adhere to the following requirements and guidelines for developing mobile applications. All requirements and guidelines are found in the *Securing Mobile Devices and Applications [CIO-IT Security-12-67 Rev. 6]*, which will be provided upon contract award.

A mobile application, most referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer. Mobile applications frequently serve to provide users with similar services to those accessed on PCs. Apps are generally small, individual software units with limited capabilities and isolated functionality. The simplest apps are developed to utilize the web browser of the mobile device to provide a feature set integration much like what is found on a user's PC. However, as mobile app development has grown, a more sophisticated approach involves developing applications specifically for the mobile environment, taking advantage of both its limitations and advantages. For example, apps that use location-based features are inherently built from the ground up with an eye to mobile devices given that you do not have the same concept of location on a PC. With this new paradigm in both mobile platforms and the applications loaded on them, GSA will concentrate security focus on the following goals:

- That all apps loaded have an initial assessment by GSA for acceptability and then a security assessment & authorization, when required.

- That all apps are deployed from only trusted sources, following their BMC systems security assessment process – This presently is the Apple iTunes store for iOS and the Google Play store for Android. MaaS360 may also be used, once retrieved from these sources, for enterprise deployment.

- That Terms of Service (ToS) discipline is adhered to, based on acceptability of an app – either as an individual user or for GSA as an Agency

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- That apps deemed to be unacceptable are blacklisted, using MaaS360.
- That a mobile app inventory for all devices be maintained
- That GSA developed apps are assessed, evaluated, and approved by the AO for the system they support before deployment.

7.0 Identification and Authentication Requirements

- The vendor shall support configurable integrations with GSA operated, and government-wide operated, identity and authentication / single sign on services. The vendor shall support SAML 2.0 and/or OpenID Connect integrations. GSA will identify and provide the services upon award.
- The vendor shall support multi-factor authentication for GSA administrator users (privileged users) through integrations with a GSA managed identity and authentication service. The vendor shall support SAML 2.0 and/or OpenID Connect integrations.

8.0 Other Security and Privacy Requirements

- Compliance with Section 889 Part A and B of the *John S. McCain National Defense Authorization Act (NDAA)*.
- No third-party integrations are authorized without the expressed permission of the GSA CISO and/or Authorizing Official and an assessment and authorization of the third-party offering having been completed prior to the integration.
- The Contractor shall comply with GSA administrative, physical, and technical security controls to ensure that all Government's security requirements are met. The Contractor is responsible for addressing any issues or concerns raised by PBS within five (5) workdays.
- Safeguarding Sensitive Data and Information Technology Resources
    - In accordance with FAR clause FAR 39.105: Privacy and GSAM clause GSAM Subpart 539.70: Requirements for GSA Information Systems, this section is included in the contract.
    - This section applies to all who access or use GSA information technology (IT) resources or sensitive data, including awardees, Contractors, subcontractors, lessors, suppliers, and manufacturers.
    - The GSA policies as identified in paragraphs (d), (e) and (f) of this section are applicable to the contract. These policies can be found at https://www.gsa.gov/directives or https://insite.gsa.gov/directives.
    - All the GSA policies listed in this paragraph shall be followed.
        - *1878.3A CIO Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices*
        - *2100.1P CIO GSA Information Technology (IT) Security Policy*
        - *2180.2 CIO GSA Rules of Behavior for Handling Personally Identifiable Information (PII)*
        - *2231.1 CIO GSA Data Release Policy*

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- *9297.2C CIO CHGE 1 GSA Information Breach Notification Policy*

- All the GSA policies listed in this paragraph shall be followed, when inside a GSA building or inside a GSA firewall.
  - *2100.2C CIO GSA Wireless Local Area Network (WLAN) Security*
  - *2104.1B CIO CHGE 2 GSA Information Technology (IT) General Rules of Behavior*
  - *2181.1A ADM Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors*
  - *9732.1E ADM Personnel Security and Suitability Program Handbook*
- The GSA Policies listed in this paragraph shall be followed. The contractor shall assume that all policies are applicable unless otherwise stipulated by the GSA Office of the Chief Information Security Officer.
  - *2101.2 CIO GSA Enterprise Information Technology Management (ITM) Policy*
  - *2105.1D CIO GSA Section 508: Managing Information and Communications Technology (ICT) for Individuals with Disabilities*
  - *2106.2A OSC GSA Social Media Policy*
  - *2107.1 CIO GSA Open Source Software (OSS) Policy*
  - *2108.2 CIO Software License Management*
  - *2160.2B CIO CHGE 4 GSA Electronic Messaging and Related Services*
  - *2160.4B CIO Provisioning of Information Technology (IT) Devices*
  - *2162.2 CIO GSA Digital Signature Policy*
  - *2165.2 CHGE 1 CIO P GSA Telecommunications Policy*
- The contractor and subcontractors shall insert the substance of this section in all subcontracts.

9.0 Relevant FAR Clauses

- FAR 552.239-70 Information Technology Security Plan and Security Authorization
- FAR 52.239-1 Privacy or Security Safeguards
- FAR 552.239-71 Security Requirements for Unclassified Information Technology Resources

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

9.2 Scope of Work Template (BAS Hardware/Software Upgrades)

Building ID – Sample Building Name
Building Automation System Upgrade Scope of Work
BAS Hardware and Software Upgrade

1.0 Background

In recent years, building systems have advanced to resemble more closely that of IT systems given the way in which they communicate both internally and externally with other systems. As such, many of the building systems inherently utilize Internet Protocol (IP) connectivity as part of their core functionality. The *GSA Technology Policy for PBS-Owned Building Monitoring and Control (BMC) Systems* mandates that all building technologies which require network or internet connectivity must utilize the GSA network. GSA's Office of Facilities Management (OFM), within the office of Public Buildings Services (PBS), in collaboration with the Public Buildings Information Technology Services (PB-ITS), within the office of the Chief Information Officer (CIO), is working to integrate the building systems onto a secure envelope, known as the Building Systems Network (BSN). This document is designed to specify the steps that will be required to complete for the network integration.

The facilities BMC systems will be upgraded to use BACnet/IP as the standard open protocol and eliminate obsolete controller hardware. The current BAS primarily communicates using proprietary protocols on slow serial networks and are composed of obsolete controllers. Project goals include:

- Increase the interoperability of devices, creating opportunities for energy and operational savings.
- Eliminate risk associated with legacy and obsolete BMC systems controllers and End of Life (EOL) components.
- Improve accessibility to operational and energy data.
- Leverage IT infrastructure to improve BMC systems reliability and performance.

2.0 Sample Scope of Work Assumptions

- Building Automation System Retrofit
- 1 - Eight (8) story building + basement
- 1 - Central chiller & boiler plant w/ VFD controlled water loops; 175 data points
- 9 - Air Handling Units (one for each floor); 40 data points each
- 340 - VAV Terminal Units (spread throughout floors); 12 data points each

3.0 General Scope

- Replace all ten Level-3 (Automation IP Level) Global Network Controllers (GNC) and applicable I/O, protocol port, or add-on modules with new GNCs. Upgrades shall include the database, modules, licenses, programming, graphics, etc. be upgraded to the latest PB-ITS remediated version of the manufacturer software.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- Replace all Level-4 (Field Level) controllers and any applicable I/O extensions. Upgrade shall include database, graphics, trends, alarms, etc. to the latest PB-ITS remediated version of the manufacturer software.

- Upgrade and reconfigure any existing database files, backups, graphics, etc. to the latest remediated version of the manufacturer software and install on a new GSA provided virtual server.

- All software licenses shall include an additional 5-year Software Maintenance Agreement (SMA) post project turnover and necessary support hours to provide software upgrades to the system and mitigate IT Security vulnerabilities during the 5-year period.

4.0 Codes and Standards

Work shall be in accordance with the following:

- NFPA 70, National Electric Code (NEC)
- Model Building Codes (Building, Mechanical, Plumbing)
- ANSI C12.20, Class 0.5
- Facilities Standards for the Public Building Service, P-100
- GSA Data Normalization for Building Automation Systems

5.0 Required IT Security Documents

- Building Technologies Technical Reference Guide Version 3.0 (latest version as of May 2024)
- Telecommunications Distribution Design Guide Version 8 (latest version as of May 2024)
- BMC Systems Security Assessment Process [CIO IT Security 16-76 Rev 4] (latest version as of May 2024)
- Key Management [CIO IT Security 09-43, Rev 5] (latest version as of May 2024)
- 2100.1P CIO GSA Information Technology (IT) Security Policy (latest version as of May 2024)
- Managing Enterprise Cybersecurity Risk [CIO-IT Security 06-30 Rev-24] (latest version as of May 2024)
- 2180.2 CIO GSA Rules of Behavior for Handling Personally Identifiable Information (PII) (latest version as of May 2024)
- 2181.1A ADM Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors (latest version as of May 2024)
- 2100.2C CIO GSA Wireless Local Area Network (WLAN) Security (latest version as of May 2024)
- IT Policy Requirements Guide [CIO-IT Security 12-2018 Rev 3] (latest version as of May 2024)
- Security and Privacy Requirements for IT Acquisition Efforts [CIO-IT Security 09-48, Rev. 7] (latest

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

version as of May 2024)

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations (latest version as of May 2024)
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 Rev. 3, Guide to Operational Technology (OT) Security (latest version as of May 2024)

6.0 Reference Documents

The following are intended to be advisory for the interpretation of the requirements in this statement of work:

- GSA New Project Smart Buildings Design and Implementation Guidelines
- GSA Data Normalization for Building Automation Systems
- Access Card Policy and Guidance Resources
- CIW – HSPD-12 Request Form

7.0 Technical and Performance Requirements

- Capacity: All BAS shall be sized to accommodate growth and should never be at maximum capacity for storage, CPU, historical trending, licenses, or users, etc. Contractor shall adhere to the 30% rule in all aspects of the BAS design. If any aspect of the system reaches 100% capacity, the contractor shall include the additional components (HW, SW, licenses, users, etc.) and/or resources to reduce the load to 70%.

- Clearances: Contractor shall comply with the requirements pertaining to mandatory HSPD-12 security clearances: The mandatory minimum security clearance level for contractor access to any GSA IT system is a Tier 1 clearance, which is a prerequisite to acquiring ENT (GSA user domain) credentials, necessary to access any GSA furnished workstation or server.

    - Per *2100.1P CIO GSA Information Technology (IT) Security Policy*, those individuals whose duties require a higher degree of trust, such as IT system administrators (or administrative access to building systems servers, applications, and devices), those who handle financial transactions, or those who deal with PII, and other sensitive information (i.e. building drawings, etc.) will require a Tier 2 clearance.

    - Within 10 days of award, contractors shall submit a CIW V4 for every member of the team who does not hold a HSPD-12 clearance.

    - Users who complete the HSPD-12 process will receive GSA ENT accounts for access to GSA hosted servers and workstations.

    - Contractor is responsible for maintaining ENT accounts for all its employees. This includes logging into account regularly, changing ENT passwords every 90 days, ensuring the mandatory GSA training is completed, on the GSA On-Line University (OLU), by due dates. Failure to comply will have an impact on CPARS/contract evaluation reviews.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- Cabling: All cabling in GSA buildings must be designed and installed in accordance with the latest version of the Building Industry Consulting Service International Inc. (BICSI) and the *GSA Telecommunications Distribution and Design Guide (TDDG)*, as it relates to Ethernet cabling.

- Schedule and Meetings: Within [X] days of contract award, the contractor's project manager shall produce a project schedule prepared in Microsoft Project or equivalent, listing all planned work activities, the duration, interdependencies, planned start and finish with a Gantt style chart. This schedule shall be continuously updated weekly until the project is complete. The project manager shall also hold a project kick-off meeting to review the schedule and update on any planned work in the upcoming weeks.

- Government Furnished Equipment (GFE): Any required computer or server hardware (i.e. PC, laptop) and peripherals (i.e. mouse, keyboard, monitor) and/or routing and switching equipment, used to provide GSA network connectivity, will be government furnished and provided by the GSA. The BAS vendor shall not include GFE, as defined, in their proposal.

8.0 Work Included

Engineering, Submittals, and IT Security Requirements:

- Contractor shall provide complete design of the proposed replacement system. Design shall include indications of devices that will be replaced, wiring diagrams of IP network, BACnet MS/TP (or other) network and I/O.

- Contractor shall provide a detailed schedule of system replacement. Schedule shall be coordinated with O&M to assure the building maintains operation throughout system replacement or work is scheduled for non-occupied hours to minimize tenant impact.

- A network riser diagram of all IP addressable devices that terminate on the GSA network shall be provided to the BTSD Technical PM, in a Microsoft Visio format. The GSA shall be included in the design phase of the network infrastructure.

- Any contractor provided hardware and software requiring access to the GSA network, must be pre-approved for use by the GSA IT.

- In accordance with OMB M-21-07, Completing the Transition to Internet Protocol Version 6 (IPv6) (2020) and GSA's Internet Protocol Version 6 (IPv6) Policy, 2120.1 CIO (2022), all new networked federal information systems must be IPv6 capable at the time of deployment. IPv4 will no longer be allowed for new projects/assessments going forward. ***Please Note: See also GSAR § 511.170(e), which requires contracting officers to include IPv6 requirements in all contracts and orders for information technology that will have the capability to access the Internet or any network utilizing Internet Protocol.***

- All IP enabled devices will be evaluated and scanned by GSA IT to determine any potential IT security vulnerabilities. The GSA IT Security Team performs security control reviews utilizing a systematic, repeatable approach, which is utilized to uniformly evaluate any device, application, or general support system. Upon completion of the security review the GSA IT Security Team can determine the extent to which the security controls associated with the device/application (information system) are implemented correctly, operating as intended, and producing the desired

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

outcome with respect to meeting the established security requirements. The GSA IT Security Team works closely with the vendor/manufacturer or the designated device POC to address specific actions taken or planned to correct deficiencies in the security controls and to reduce or eliminate known vulnerabilities in the information system. Upon successful completion of the security review, the GSA will have the information needed to determine the risk to agency operations, agency assets, or individuals and thus, will be able to render an appropriate security decision for the information system. Contractors **must** make any required configuration changes before their product will be accepted for use. Configuration changes are not a change in scope and are not subject to equitable adjustment under the contract. The contractor must provide reasonable assurance to the GSA that all applicable system specific security controls are in place prior to implementing the given IT application or system, in a production environment. It is incumbent upon the vendor selected to review and understand the government and the GSA IT security requirements. Failure to meet the GSA IT requirements will be subject to liquidated damages.

- At no time should a GSA hosted BMC system(s) be made accessible to the public internet or via any 3rd party network connection, referred to as “rogue circuits”. All network traffic must transit through a trusted internet connection (TIC), which is a network circuit that is managed by the GSA IT. Any use of external/commercial network connection for managing or monitoring of building systems in any GSA owned or non-delegated building will not be tolerated. Such connections will be removed upon discovery and will negatively impact the vendor’s performance rating.

- Any Contractor proposed non-standard software must be pre-approved by GSA IT before it is deployed. "Nonstandard software" is defined as software which is not widely dispersed and commercially available on GFE. The GSA will **not** accept the use of legacy technologies or systems such as:

    - Hardware-based USB/dongle licensing (software licensing should be used)
    - Applications that require Java (should use HTML 5.0)
    - Use of local accounts (non-Active Directory) on servers for applications to function or be used.
    - Use of additional embedded virtual machines
    - Proprietary protocols that cannot be remediated
    - Software that requires elevated privileges for operation (i.e. super-user or administrator)

- All proposed standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved United States Government Configuration Baseline (USGCB).

- All software licenses are to be titled to the GSA and shall not be under the BAS vendor’s ownership.

- Any contractor proposed software solution shall require minimal administrative rights at the operating system (OS) level. Administrative rights shall be limited for software installation, updates, patching, and in unique cases such as for troubleshooting issues. For day-to-day operations, the application will run with normal user level rights. ***Please Note: This is not in reference to full rights to the application itself, only elevated rights to the root level of the operating systems.***

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- Upon completion of the project, all licenses purchased shall have all rights and permissions transferred to the GSA to manage, edit, and move at its discretion. The GSA retains all ownership and licenses purchased should reflect the GSA as owner where necessary.

- BAS software shall be loaded onto GSA-provided virtual servers. This configuration allows for flexibility in access and system control over the BSN.

- Incident response (IR) and building recovery (BR) exercises - Since BMC Systems that reside on the GSA network rely on IP network communications and computer hardware, they are subject to the impacts associated with interruptions in service of that IT infrastructure. To prepare GSA facility's BMC System in the event of a data circuit failure, Local Area Network (LAN) outage, cyber-attack or application server failure, BR preparations need to be planned and tested.

    - IR entails the contractors' ability to identify a potential cyber incident and the ability to immediately report the issue to GSA IT [redacted] An incident is a violation or an imminent threat of violation of information security or privacy policies, acceptable use policies, or standard security practices.

    - An effectively developed BR plan will ensure that while network communications may be temporarily unavailable, building control system components will continue to function, and in fact may also be programmable if local software-based tools are available, ensuring that building operations will not be significantly impacted. This means the BMC systems contractor will need to document and submit operational procedures to monitor and control systems in case of an outage, to ensure continuity of operations, as part of the commissioning process. Once the plan is developed, a BR exercise will be conducted where an IT outage is simulated. The exercise can consist of limiting the ability of IP based controllers to communicate to the application server and/or to other parts of the network. Executing the BR exercise will require coordination and participation from Facility Management, Operations and Maintenance and GSA IT. Contractor shall submit BR operational procedures in case of wide area network (WAN) connection loss. BR procedures shall ensure continued operation of the system in cases of network loss and shall instruct operators how to monitor and control systems in cases of internet outages.

    - To meet the requirements of the Smart Building Design Standards, all building system data points must be exposed on the GSA network for future third-party integration. Proposed controls systems must include the ability to transfer data to a third-party via an automated data push or third-party initiated query using an open and published methodology including, but not limited to, BACnet/IP, oBIX, OPC, Haystack, ModbusTCP etc. The contractor shall document a proposed means of data transfer for this system.

Building Automation System Installation and Configuration:

- Where new programming and point mapping must be completed, Contractor shall adhere to the supplied "GSA Data Normalization for Building Automation Systems" document for standard point naming conventions and tagging requirements for GSA systems.

- Contractor shall replace all existing Global Network Controllers, I/O modules (and 3rd Party Modules), or protocol port modules with new hardware and include necessary database conversions, programming, graphics, and historical trending.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- Contractor shall ensure that all new hardware is configured with the latest GSA IT remediated Software and Firmware and hardened per the SAR guidelines.

- Contractor shall install and license the latest GSA IT remediated version of the Building Automation System Software on a GSA provided Virtual Machine and migrate/upgrade the existing BAS Database to the new server. BAS Software will be required to run (at minimum) on Windows Server 2019 (or latest Operating Systems approved by GSA IT). BAS Software must be supported by the manufacturer on the designated Server OS. All licenses for BSN console software licensing or other device configuration tools for local controllers acquired through projects must be in GSA's name.

- Replacement controllers and software shall be configured to utilize existing devices and sequences as currently utilized in the existing BAS. Contractor shall document sequences before and after system migration and provide a list to the GSA of any I/O found not in working order prior to replacing controllers.

- Contractor shall work with the building O&M personnel to determine and provide a list of overridden points within the system prior to cutover and ensure any existing overrides are enabled or re-enabled after cutover to ensure proper building operation.

- At the time of "Cut Over," the existing BMC network unmanaged switches (if applicable) shall be removed, replaced with Government Furnished Switches, all network terminations shall be made, and each IP enabled device shall be migrated. Upon completion of work, documentation of any deviations shall be made on the record drawing set and published. GSA IT will request various forms to be completed documenting the project which must be completed and provided within 5 business days of the cutover.

- Every IP level device shall be configured to the proper GSA IT Building System Network IP address as directed by GSA IT. The BACnet/Ethernet communication protocol is not permitted on the GSA network so BACnet/IP must be implemented as the communication protocol.

- IP addresses for all BAS IP level devices will be issued and distributed by BTSD after receiving the make, model, MAC address of each IP device (to be whitelisted), and the inspection and approval of the network diagram.

- Contractor shall be responsible for configuring any BACnet, UDP or TCP traffic between controllers, servers, and clients to prevent broadcast "storms" or "collisions" or any other network disruptions. This may include installing and configuring a BBMD or reconfiguring BACnet ports to a specified port as directed by the GSA.

- Contractor shall provide necessary testing and documentation showing that the system has been successfully transferred to the new GSA provided Server.

Building Automation Network Configuration (Pre-Migration):

- The BAS network shall comply with the GSA TDDG, specifically distance and network hop limits. Fiber or copper connections from the core switch to risers shall prevent "daisy chaining" of network switches.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- Contractor shall be responsible for connecting the Building Automation Network core switch and GSA Network demarcation.

Building Automation System Cutover (Migration):

- Upon completion of all pre-migration work and after receipt of the government furnished network switches (if necessary), the BMC systems contractor shall coordinate a date to “Cut Over,” the BMC System from the existing server and onto the new BMC systems server. The BMC systems contractor shall prepare a detailed procedure of all planned work activities, pointing out possible risks and impact to the building of all work. A risk management plan to identify risks with a planned procedure of steps to be taken if such a risk event arises shall be presented and discussed with all team members.

- At the time of “Cut Over,” all necessary network terminations shall be made, and each IP enabled device shall be migrated. Upon completion of work, documentation of any deviations shall be made on the record drawing set and published. The GSA IT department will request various forms to be completed documenting the project which must be completed and provided within 5 business days of the cutover.

- The BAS contractor shall be required to confirm communication and functionality after completion of a GSA network integration, including device to device and device to server.

- The BAS contractor/cabling vendor is responsible for all cabling to BAS controllers, GFE switches and BSN Workstations (if applicable).

- At the completion of the “cut over,” the old controllers, and any unused wiring/cabling component of the BMC System shall be wiped and removed from the building, following GSA’s excess process, by the contractor.

- At the completion of the system migration, the contractor shall complete the SAR Hardening Verification form. A member from the BMC Security Assessment Team will reach out if any hardening steps have not been completed and the contractor must take corrective actions to resolve any outstanding hardening steps.

- At completion of the system migration, the contractor shall coordinate and verify a BR operation exercise Facility Management and Operations and Maintenance staff present. This exercise shall ensure continued operations and emergency system maintenance procedures in cases of network loss.

9.0 Software Maintenance Agreement (SMA)

- Contractor shall provide an additional 5-year (SMA), that begins post project turnover, and include the necessary support hours to provide software upgrades to the system and mitigate any future IT Security vulnerabilities.

- SMA shall include minor and major software/firmware releases to all BAS software and hardware as defined by the GSA.

- All firmware/software versions must be remediated and approved by GSA IT and installation

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

coordinated through the GSA Facility Management Team at the building.

- Upgrades shall be performed within timeframes agreeable to GSA to mitigate risk and/or downtime to the GSA facility.

- For any BMC systems device that is a Windows or Linux based Operating System, the Contractor will sign an agreement between the vendor and GSA adhering to patching monthly. The Contractor will be responsible for patching the devices monthly.

10.0 Work Not Included

- Costs for providing internal GSA security escort and technical personnel.

- GSA shall ensure a connection to the GSA LAN is present and functioning.

- GSA shall provide all network switches, servers, workstations, and peripherals.

11.0 Warranty

Provide information of the manufacturer’s warranty including date of commissioning/startup, points of contact, 2 years parts and labor of all components and software.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Chapter 10

Best Practices for BMC Systems Project Implementations

10.0 Overview

This chapter entails best practices for integration of BMC Systems to the GSA network.

10.1 Tips for Running a Successful BMC Systems Project

- Contact the appropriate project representative during the preparation and planning stages of the project. This will ensure that the solution is compliant with GSA IT security and network connectivity requirements. Potential Stakeholders include:
    - BTSD IT PM
    - Facility Manager (Contact the local GSA POC)
        - The onsite GSA facility managers must be involved from start to finish. Their input is imperative as it could change daily operations affecting multiple federal agency tenants.
        - Do they need to consult any clients in advance for feedback on operations, or for their early awareness on project planning? (i.e. thermostat inside judge's chambers requiring access or noise concerns)
    - Project Managers (i.e. Design and Construction, Facility Management, Service Center)
    - Contracting Officer and Contract Specialist - Consider use of the national BAS BPA. Contact regional Energy/Smart Buildings SMEs for details and share with the Regional Acquisition Team.
    - Client Representative
    - Operations and Maintenance (O&M) Contractors, Master Systems Integrators (MSIs), Energy Saving Performance Contractors (ESPC) or Utility Energy Saving Contractors (UESC) Contractors - Contact local operators to document concerns on the system.
        - What do they know about the needs of the building or system?
        - Based on their backgrounds, will a more advanced system be a potential issue even after training?
    - PBS Smart Buildings Intelligent Building Industry Experts (IBIEs)
    - Regional Facility Management Smart Building Subject Matter Experts (SMEs)

    Considerations for Scope of Work Development

    - Ensure security language and GSA IT requirements are included in the scope of work (SOW) of

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

the procurements. ***Please Note: See Section 9.2 for more details.***

- Interoperability
  - Strive for a cohesive system with interoperability capabilities (i.e. advanced metering, national digital signage (NDS), GSALink, etc.)
  - Consider conducting building system analysis or review to plan for compatibility across systems for controls.
- Technical Considerations for Requirements
  - Device naming standards, BAS account creation process and account naming standards must be implemented.
  - If using the BACnet protocol, ensure the contractor is not using the default User Datagram Protocol (UDP) port number for 47808. Regional PBS stakeholders need to ensure they assign UDP ports that have been assigned to their respective regions. Essentially, this allows each region to take the initiative to protect itself from potential BACnet conflicts with systems in other regions. Please work with the BTSD Technical PM to access UDP port assignments.
  - Consideration for special operations, systems, or clients. Are there unique mechanical systems onsite or client impacts based on noise or operations for the project? (i.e. glycol systems, geographically challenging locations, unique clients/tenants). Does the facility operate 24/7 or support large computer/data/server centers?
  - What is the big picture? Are there other upcoming projects that would align the major building equipment? Can timelines be aligned? Investigate equipment onsite to ensure it is operational and has substantial (10+ years) remaining prior to attempting integration without consultation to all stakeholders. Work with the regional Portfolio Manager to obtain plans or details for the facility.
  - Special Licensing Requirements - All licenses for BSN console software licensing or other device configuration tools for local controllers acquired through projects must be in GSA's name.
  - Include requirements for advanced notice to stakeholders regarding the scheduling of Control System Switch over.
  - END OF LIFE (EOL) - Require Dates for EOL equipment/software. This is helpful for decisions on partial system replacement VS full system replacement. Require dates of EOL for equipment so that it can be vetted by region for decisions on partial system renovations vs full system replacements.
  - WARRANTY PERIOD - Are there any special warranty period commencement requirements? Define regional minimums within the task order.
    - Ensure contracts include a 5-year software SMA, that begins post project turnover, and include the necessary support hours to provide software upgrades to the system and mitigate any future IT Security vulnerabilities. Potential Language: *"Service Maintenance Agreements (SMAs) for software subscriptions shall be a minimum of 5 years and shall include all labor, associated travel and expenses for a minimum of 1 year (tracking warranty*

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

period) from GSA acceptance of a project."

- Be certain that a warranty of the devices, patching and security updates are included as part of the scope of work.

- Training - Implement a GSA user training for the O&M as part of the project closeout. Are there any special training requirements? Items for consideration to include in requirements:
  - Specifics on training date coordination.
  - Format of Training.
  - Topics & documentation on using the system.
  - Remote access & building recovery procedures.
  - How to contact GSA IT.
  - and/or review of any final deliverables.
- Make sure to have COOP planning in place and perform a BR exercise. Ensure controllers have appropriate settings.
  - Have an ability to directly connect to the controllers to manually control the system. Doing this should allow the system to be managed locally, in the event of an outage, if/when the server is not accessible.
  - Conduct a BR exercise to make sure the O&M can control the system in the event of an outage.

- Post Implementation Delivery Recommendations
  - Remind facility managers and O&M to consult regional program SMEs before implementing any changes to maintenance plans. Example: O&M contractor decided to stop using chemicals in the cooling towers and instead pressure wash it regularly at a newly constructed Federal Courthouse. This resulted in damage to the media fins in the cooling towers which broke off and got sucked into the circulating pumps causing multiple problems.
  - Document lessons learned to share with regional and national network peers.
  - Update Contractor Performance Assessment Reporting System (CPARS) to help support evaluation of future contractors for GSA.
  - Ensure network access (ENT) is maintained for the project staff:
    - Logging into the network at least every 60 days.
    - Changing ENT password every 90 days.
    - Taking the annual mandatory training on the GSA OLU.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

10.2 BMC Systems Checklist for Projects

Before the cutover, defer to the best practices of the O&M contractor and industry standards to verify that the system is functioning properly.

10.2.1 Unitary Controller Configuration

- Verify types of networks, and number of field devices agree with submittals.
- Verify field networks are operational.
- Verify field devices are operational on the network.
- Verify that any points, objects, programming wizards, tools, etc. that are associated with manufacturer specific modules or JAR files are operational.
- Compare Sequence of Operation to logic program provided by BMC systems Integrator/Contractor. Sequences shall automatically lead/lag equipment when equipment or hardware failure occurs.
- Provide record that 30% spare capacity remains on the DDC controllers for future expansion of the system as required by the P-100.
- Verify unitary network controllers operate at last known <fail safe> state by shutting the global controller down and observing the plant or AHUs.
- Verify unitary network controllers <fail safe> occupied when the loose heartbeat from the supervisory global controller with the schedules.

10.2.2 Server/AMS Configuration

- Global Controllers are required to be networked TCP/IP to regional AMS Schneider PME Server.
- Global Controllers are required to be provisioned for automatic backup (if applicable) to BMC systems servers.
- The Alarm Recipient (Server) shall route alarms properly.
- AMS points are required to be shared from the BMC systems global controller metering graphic page.
- AMS points are required to be mapped to AMS Server.

10.2.3 General Documentation and Deliverables

- Provide Global controller license files.
- Back up all BMC systems project deliverable files on Google Drive. If the server is used to store backups, work with the TechOps Server Team to identify an appropriate/dedicated location server so that it can be backed up properly.
- Update MS Visio Riser Diagram.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

- 100% Points Commissioning Document provided to the GSA SOW.
- Send designated Global Controller names and IP addresses.
- Provide updated “as-built” control drawings and points list.
- Complete a Building Recovery Plan, if applicable.

10.2.4 Application Account Administration

- Use of vendor established administrative level usernames and passwords to be provided by the GSA or provided to the GSA upon completion of the project.
- The vendor shall not establish any administrative level usernames or passwords that would otherwise lock out the GSA from their own systems.
- The vendor shall understand that in certain instances some regional POC will issue & control all passwords for use on a project along with account expiration dates. Vendors cannot alter their usernames or expiration dates.
- Prior to adding additional user accounts in applications and/or hardware, the vendor must seek permission from the SME POC/BTSD Technical PM and provide the details of what accounts would be created so that the GSA is aware of each user and permission level the user will have.
- Sensitive handling measures must take place in transmitting Controlled Unclassified Information (CUI) information. All CUI information must use secure transmission channels, and by using GSA.gov domain email address.

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Appendix

Appendix A: Contact Information

Appendix B: Listing of Reference Policies

Document Name	Link
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-213A, IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog	https://csrc.nist.gov/pubs/sp/800/213/a/final
2100.1P CIO GSA Information Technology (IT) Security Policy	https://www.gsa.gov/directives-library/gsa-information-technology-it-security-policy-16
Federal Acquisition Regulation (FAR) Part 45	https://www.acquisition.gov/far/part-45
Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors	https://www.dhs.gov/homeland-security-presidential-directive-12
BMC Systems Security Assessment Process [CIO IT Security 16-76 Rev 4]	https://www.gsa.gov/policy-regulations/policy/information-technology-policy/it-

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Document Name	Link
	security-procedural-guides
2100.2C CIO GSA Wireless Local Area Network (LAN) Security	https://www.gsa.gov/directives-library/gsa-wireless-local-area-network-wlan-security
FIPS 140-2	https://csrc.nist.gov/pubs/fips/140-2/upd2/final
P100: Facilities Standards for the Public Buildings Service	https://www.gsa.gov/real-estate/design-and-construction/engineering/facilities-standards-for-the-public-buildings-service
ASME A17.1-2022: Safety Code for Elevators and Escalators	https://blog.ansi.org/asme-a17-1-2022-safety-code-elevator-csa-b44/
Telecommunications Distribution Design Guide Version 8	https://insite.gsa.gov/services-and-offices/staff-offices/office-of-gsa-it/it-organizations/office-of-the-deputy-cio/office-of-public-buildings-it-services/building-technology-services-division/library-of-documentation-guidance-and-resources?term=TDDG
FIPS 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors, and Federal Identity	https://csrc.nist.gov/pubs/fips/201-2/final
Office of Management and Budget (OMB) Memorandum (M-19-17)	https://www.whitehouse.gov/omb/information-for-agencies/memoranda/
GSA Order ADM 5900.1	https://www.gsa.gov/directives-library/physical-access-control-systems-in-us-general-services-administration-controlled-space
NIST SP 800-145: The NIST Definition of Cloud Computing	https://csrc.nist.gov/pubs/sp/800/145/final
Security and Privacy Requirements for IT Acquisition Efforts [CIO-IT Security 09-48, Rev. 7]	https://insite.gsa.gov/employee-resources/information-technology/it-security-and-privacy/it-security/it-security-procedural-guides
Managing Enterprise Cybersecurity Risk [CIO-IT Security 06-30 Rev-24]	https://insite.gsa.gov/employee-resources/information-technology/it-security-and-privacy/it-security/it-security-procedural-guides
Office of Management and Budget (OMB) Memorandum 21-07 (M-21-07)	https://www.whitehouse.gov/omb/information-for-agencies/memoranda/
Internet of Things Cybersecurity Improvement Act of 2020	https://www.congress.gov/bill/116th-congress/house-bill/1668
Office of Management and Budget (OMB) Memorandum (M-24-04)	https://www.whitehouse.gov/omb/information-for-agencies/memoranda/
NIST SP 800-213: IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements	https://csrc.nist.gov/pubs/sp/800/213/final
Securing Mobile Devices and Applications [CIO-IT Security-12-67 Rev. 6]	https://insite.gsa.gov/employee-resources/information-technology/it-security-and-privacy/it-security/it-security-procedural-guides
John S. McCain National Defense Authorization	https://www.acquisition.gov/Section-889-Policies

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Document Name	Link
Act (NDAA) (Section 889 Part A and B)	
1878.3A CIO Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices	https://www.gsa.gov/directives-library/developing-and-maintaining-privacy-threshold-assessments-privacy-impact-assessments-privacy-act-notices-and-system-of-records-notices-3
2180.2 CIO GSA Rules of Behavior for Handling Personally Identifiable Information (PII)	https://www.gsa.gov/directives-library/gsa-rules-of-behavior-for-handling-personally-identifiable-information-pii-2
2231.1 CIO GSA Data Release Policy	https://www.gsa.gov/directives-library/gsa-data-release-policy-2
9297.2C CIO CHGE 1 GSA Information Breach Notification Policy	https://www.gsa.gov/directives-library/gsa-information-breach-notification-policy-5
2100.2C CIO P GSA Wireless Local Area Network (LAN) Security	https://www.gsa.gov/directives-library/gsa-wireless-local-area-network-wlan-security
2104.1B CIO CHGE 2 GSA Information Technology (IT) General Rules of Behavior	https://www.gsa.gov/directives-library/gsa-information-technology-it-general-rules-of-behavior-4
2181.1A ADM Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors	https://insite.gsa.gov/directives-library/homeland-security-presidential-directive12-personal-identity-verification-and-credentialing-and-background-investigations-for-contractors-21811-adm
9732.1E ADM Personnel Security and Suitability Program Handbook	https://www.gsa.gov/directives-library/personnel-security-and-suitability-program-handbook
2101.2 CIO GSA Enterprise Information Technology Management (ITM) Policy	https://www.gsa.gov/directives-library/gsa-enterprise-information-technology-management-itm-policy-1
2105.1D CIO GSA Section 508: Managing Information and Communications Technology (ICT) for Individuals with Disabilities	https://www.gsa.gov/directives-library/gsa-section-508-managing-information-and-communications-technology-ict-for-individuals-with-disabilities-1
2106.2A OSC GSA Social Media Policy	https://www.gsa.gov/directives-library/gsa-social-media-policy-2
2107.1 CIO GSA Open Source Software (OSS) Policy	https://www.gsa.gov/directives-library/gsa-open-source-software-oss-policy-1
2108.2 CIO Software License Management	https://www.gsa.gov/directives-library/software-license-management-1
2160.2B CIO CHGE 4 GSA Electronic Messaging and Related Services	https://www.gsa.gov/directives-library/gsa-electronic-messaging-and-related-services-3
2160.4B CIO Provisioning of Information Technology (IT) Devices	https://www.gsa.gov/directives-library/provisioning-of-information-technology-it-devices-2
2162.2 CIO GSA Digital Signature Policy	https://www.gsa.gov/directives-library/gsa-digital-signature-policy
2165.2 CHGE 1 CIO P GSA Telecommunications Policy	https://www.gsa.gov/directives-library/gsa-telecommunications-policy-1

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

Document Name	Link
GSA Technology Policy for PBS-Owned Building Monitoring and Control (BMC) Systems	https://insite.gsa.gov/services-and-offices/public-buildings-service/facilities-management/facility-technology-innovation/technology-guidance?check_logged_in=1
Key Management [CIO IT Security 09-43, Rev 5]	https://insite.gsa.gov/employee-resources/information-technology/it-security-and-privacy/it-security/it-security-procedural-guides
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 Rev. 3, Guide to Operational Technology (OT) Security	https://csrc.nist.gov/pubs/sp/800/82/r3/final

Appendix C: Change Log

Revision	Chapter	Change
Revision 1.1	1	TIC
	1	Formal Security Evaluation
	1	Security Evaluation Criteria
	1	Devices Risk Assessments
	1	Scanned Device List
	1	Client Software (Non-Standard Software)
	1	Non-Standard Software on GSA Servers
	1	GSA-IT Security Scanning Process
	1	Building Systems Network (BSN)
	2	BACnet
	3	Cabling Installation Options

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	3	Overview of Data Circuit Installation
	4	Responsibilities Respective to Server and Application Support
	4	Server Installation Guidelines
	4	Methods for Remotely Accessing a PBS Technical Operations Server
	4	System Documentation and Monitoring
	4	Backup Solutions
	4	Planned/Unplanned Outages and Maintenance
	6	Reporting an BMC Issue
	6	BMC Support System Workflow
	7	PACS (New Chapter)
Revision 1.2	1	Introduction
	1	Scanning Process
	1	What is BSN?
	2	Issues with Daisy Chaining Switches
	4	Solution Architecture and Requirements Analysis
	4	Server Standards
	4	Application Installation and Maintenance Guidelines
	4	Server Access
	4	Methods for Remotely Accessing a PBS Technical Operations

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

		Server
	4	System Documentation and Monitoring
	4	How to Request Remote Desktop User Access
	4	How to Request Administrator Access
	4	Copying Files to a Server on the BSN
	4	Methods for Remotely Accessing a PBS Technical Operations Server
	5	New SOW format and language
	6	Reporting a BMC Issue
	6	PBS Technical Operations Team
	6	BMC Outage Process
	6	BMC Admin, RDP, and Reboot Process
	6	SFTP (Secure File Transfer Protocol) Request Process
	6	SMTP Email Server Information
	8	Best Practices (New Chapter)
Revision 2.0	Introduction	Updated Introduction
	1	Updated Section 1.1 “Roles and Responsibilities”
	1	Moved and Updated Section 1.2 “Policies and Requirements for Interconnectivity”
	1	Moved and Updated Section 1.2.1 “Trusted Internet Connection (TIC)”

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	1	Added Section 1.2.2 “Cellular Connection”
	1	Added Section 1.2.4 “BMC Whitelisting Process”
	1	Moved and Updated Section 1.3 “GSA Network Access to Perform Duties”
	1	Removed Section 1.3.2 “Server Security Assessment”
	1	Removed Section 1.3.3 “Device Security Assessment”
	1	Updated Section 1.4 to reflect the entire “BMC Device and Application Security Assessment Process”
	1	Added Section 1.4.1 “IT Security Scanning Process” Wireless Assessments
	1	Added Section 1.4.2 “Wireless Assessments”
	1	Added Section 1.4.3 “Encryption”
	1	Moved and Updated Section 1.4.4 “Non-Standard Software Review Process (BSN Servers/ Consoles)”
	1	Moved and Updated Section 1.5 “Building Systems Network (BSN)”
	1	Updated Section 1.5.1 “What is the Building Systems Network (BSN)?”
	1	Removed Section “Why is the BSN Necessary?”
	1	Updated Section 1.5.2 “BSN Operations and Maintenance Roles and Responsibilities”
	1	Updated Section 1.5.3 “BSN Evolvement and Implementation”
	1	Added Section 1.5.3.1 “BSN I: ACLs and Dedicated VLANs”
	1	Added Section 1.5.3.2 “BSN II: Dynamic Multipoint Virtual Private Network (DMVPN)

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	1	Added Section 1.5.3.3 “BSN III: Software-Defined Wide Area Network (SD-WAN)”
	1	Added Section 1.5.3.4 “BSN IV: Trustsec and Microsegmentation”
	1	Updated Section 1.5.4 “Expected Changes Once the BSN ACL is Applied”
	1	Updated Section 1.5.5 “How to Access Virtual Servers in BSN”
	1	Updated Section 1.5.6 “BSN Consoles”
	1	Added Section 1.5.6.1 “How to Obtain a BSN Console”
	1	Moved and Updated Section 1.5.6.2 “How to Access a BSN Console”
	1	Moved and Updated Section 1.5.6.3 “Installing Software on the BSN Console”
	1	Moved and Updated Section 1.5.9 “Steps to Integrate Sites onto the BSN from the ENT Domain”
	1	Moved and Updated Section 1.5.9.1 “Preparation”
	1	Moved and Updated Section 1.5.9.2 “BSN Preparation Meeting/Training”
	1	Moved and Updated Section 1.5.9.3 “Citrix-VDI Access and Use”
	1	Moved and Updated Section 1.5.9.4 “Migration”
	1	Disaster Recovery Changed to Building Recovery
	1	Moved and Updated Section 1.6 “Incident Response (IR) and Building Recovery (BR) Exercises”
	1	Moved and Updated Section 1.6.1 “Incident Response”
	1	Moved and Updated Section 1.6.2 “Building Recovery Exercises”

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	2	Updated Overview
	2	Updated Section 2.1 “Network Roles and Responsibilities”
	2	Removed Figure 2-1 “GSA MPLS Logical Backbone”
	2	Moved Section 2.2 “GSA Network and Uptime” from Best Practices Chapter
	2	Updated Section 2.4.1 “Network Design Requirements”
	2	Updated Section 2.4.2 “Sample Network Design Diagrams” with an updated sample of an acceptable network design diagram
	2	Moved Section 2.5 to 2.4.3 “Acceptance of Non-Standard Hardware”
	2	Added Section 2.5.1 “Requesting a GSA Circuit”
	2	Moved Section 2.5.1 to 2.5.2 “Requesting Switches and Routers”
	2	Moved Section 2.5.2 to 2.5.3 “Configuration and Connection of the Switches and the Routers”
	2	Moved Section 2.5.3 to 2.5.4 “Acceptance of Non-Standard Hardware”
	2	Moved and Updated Section 2.6 “BACnet”
	2	Updated Section 2.6.1 “How Does a BACnet Make Use of IP Networks?”
	2	Updated Section 2.6.2 “BACnet Key Definitions”
	2	Removed “Implementing BACnet on a Local Area Network (LAN)”
	2	Updated Section 2.6.3 “Implementing BACnet on a Wide Area Network (WAN)”
	2	Updated Section 2.6.3.1 “UDP Port Assignment”

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	2	Updated Section 2.6.3.2 “BACnet/Ethernet”
	2	Moved and Updated Section 2.6.3.3 “Using a BACnet Broadcast Management Device (BBMD)”
	2	Moved and Updated Section 2.6.3.4 “Foreign Device Registration”
	2	Moved and Updated Section 2.6.3.5 “BACnet/IP Multicast (B/IP-M)”
	3	Updated Overview
	3	Updated Section 3.1 “Applicable Standards for Cabling Infrastructure”
	3	Moved and Updated Section 3.1.1 “Minimum Requirement for Ethernet Cabling”
	3	Moved and Updated Section 3.1.2 “Attenuation Limit”
	3	Moved and Updated Section 3.1.3 “How are GSA-IT’s Cabling Standards Enforced?”
	3	Moved and Updated Section 3.2 “Cabling Installation”
	3	Moved and Updated Section 3.2.1 “Cabling Installation Roles and Responsibilities”
	3	Moved Section 3.2.2 “General Architecture”
	3	Moved and Updated Section 3.2.3 “Cable Installation Options”
	3	Moved and Updated Section 3.2.4 “Cable Installation Support”
	3	Moved and Updated Section 3.3 “Data Circuit Installation”
	3	Moved and Updated Section 3.3.1 “Data Circuit Installation Roles and Responsibilities”
	3	Moved and Updated Section 3.3.2 “Process for Data Circuit Requests and Site Visits”

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	3	Moved and Updated Section 3.3.3 “Important Considerations in the Circuit Installation Process”
	4	Updated Overview
	4	Updated Section 4.1 “BMC Server Roles and Responsibilities”
	4	Moved and Updated Section 4.2 “BMC Server Standards”
	4	Moved and Updated Section 4.2.1 “Why Go Virtual?” from Best Practices Chapter
	4	Moved and Updated Section 4.2.2 “BMC Server Hardware and Software Specifications”
	4	Moved and Updated Section 4.2.3 “BMC Application Requirements”
	4	Moved and Updated Section 4.2.4 “Server Security Hardening”
	4	Moved and Updated Section 4.3 “BMC Deployment Process”
	4	Added Section 4.3.1 “Step 1: Submit BMC Server Request Form”
	4	Added Section 4.3.2 “Step 2: Schedule Server Solutions Meeting with TechOps”
	4	Added Section 4.3.3 “Step 3: Server Deployment Process”
	4	Moved and Updated Section 4.4 “Application Installation and Maintenance Guidelines”
	4	Moved and Updated Section 4.4.1 “Installation and Maintenance Roles and Responsibilities”
	4	Moved, Renamed and Updated Section 4.4.2 “Do’s and Don’ts for Application Instructions”
	4	Moved Authority Approval Table from Chapter 6 to Chapter 4 Section 4.4.4
	4	Updated Section 4.4.5 “Dedicated Server Support During

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

		Installation”
	4	Added Section 4.4.6 “Copying Files to a Server on the BSN”
	4	Moved and Updated Section 4.4.6 with The Secure File Transfer Protocol (SFTP) Request Process
	4	Moved and Updated Section 4.4.7 “Simple Mail Transfer Protocol (SMTP) Email Server Information” from Chapter 6 to Chapter 4
	4	Moved and Updated Section 4.5 “Application Access”
	4	Added Section 4.5.1 “Methods for Accessing an Application via Web Browser”
	4	Added Section 4.5.1.1 “How to Request Access to a Web Application”
	4	Added Section 4.5.1.2 “How to Access a Web Application via Citrix VDI”
	4	Added Section 4.5.1.3 “How to Access a Web Application via BSN Console”
	4	Moved and Updated Section 4.5.2 “Methods for Accessing an Application via RDP to a Server”
	4	Moved and Updated Section 4.5.2.1 “How to Request RDP Access to a Server”
	4	Moved and Updated Section 4.5.2.2 “How to RDP to a Server via Citrix VDI”
	4	Moved and Updated Section 4.5.2.3 “How to RDP to a Server via BSN Consoles”
	4	Added Section 4.5.2.4 “How to Log Off a Remote Desktop Session on a BMC Server”
	5	Moved Chapter 6 to Chapter 5 “Technical Support for BMC Servers and Consoles”
	5	Updated Overview

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	5	Moved and Updated Section 5.1 “Technical Support Roles and Responsibilities”
	5	Moved and Updated Section 5.2 “Server Maintenance and Support” from Chapter 4 to Chapter 5
	5	Moved and Updated Section 5.2.1 “Server Monitoring” from Chapter 4 to Chapter 5
	5	Added Section 5.2.2 “Server Backup Solutions”
	5	Moved and Updated Section 5.2.3 “Server Patching” from Chapter 4 to Chapter 5
	5	Combined and Updated Section 5.3.2.1 “Planned Maintenance and Outages” from Chapter 4 and Chapter 6 to Chapter 5
	5	Combined and Updated Section 5.3.2.2 “Unplanned Maintenance and Outages” from Chapter 4 and Chapter 6 to Chapter 5
	5	Moved and Updated Section 5.2.4 “Communications for BMC Contacts” from Chapter 5 to Chapter 5
	5	Added Section 5.3 “BSN Console Maintenance”
	5	Added Section 5.3.1 “BSN Console Patching”
	5	Added Section 5.3.2 “BSN Console IT Support”
	5	Moved and Updated Section 5.4 “BMC Issue”
	5	Added Section 5.4.1 “Initial Troubleshooting Steps”
	5	Added Section 5.4.2 “Different Methods of Reporting a BMC Issue”
	5	Added Section 5.4.2.1 “Option 1: Call TechOps”
	5	Added Section 5.4.2.2 “Option 2: Email TechOps”

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	5	Moved and Updated Section 5.4.2.3 “Option 3: Call the GSA-IT Service Desk Hotline”
	5	Moved and Updated Section 5.4.2.4 “Option 4: Submit a GSA-IT Service Desk Ticket with ServiceNow”
	5	Moved and Updated Section 5.4.2.5 “Describing a BMC Issue”
	5	Added Section 5.4.3 “BMC Support System Workflow”
	5	Added Section 5.4.3.1 “BMC Application Issue”
	5	Added Section 5.4.3.2 “Network Issue”
	5	Added Section 5.4.3.3 “BMC Server Issue”
	5	Added Section 5.4.3.4 “BSN Console Issue”
	5	Added Section 5.4.3.5 “Advanced Metering System (AMS) Issue”
	5	Added Section 5.4.3.6 “Troubleshooting Points of Contact”
	6	Added Chapter 6 “Advanced Metering System (AMS)”
	7	Updated Overview
	7	Moved and Updated Section 7.1 “Physical Access Control Systems Roles and Responsibilities”
	7	Moved and Updated Section 7.2 “Security”
	7	Moved and Updated Section 7.3 “Network Architecture and Integration”
	7	Moved and Updated Section 7.4 “Project Flow”
	7	Moved and Updated Section 7.5 “Support”
	8	Moved Chapter 5 to Chapter 8 “IT Requirements in Scope of Work (SOW) for BMC Procurements”

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	8	Updated Section 8.0 Overview
	8	Updated Section 8.1 “Scope of Work Template (BAS Hardware/Software Upgrades)”
	9	Moved Best Practices from Chapter 8 to Chapter 9
	9	Updated Overview
	9	Moved and Updated Section 9.1 “Tips for Running a Successful BMC Project”
	9	Added Section 9.2 “BMC Checklist for Projects”
	9	Added Section 9.2.1 “Unitary Controller Configuration”
	9	Added Section 9.2.2 “Server/AMS Configuration”
	9	Added Section 9.2.3 “General Documentation and Deliverables”
	9	Added Section 9.2.4 “Application Account Administration”
	Appendix	Combined Appendix into 1 List
	Appendix	Appendix A: Updated Contact Information
	Appendix	Appendix B: Listing of Reference Policies
Revision 3.0	Introduction	Updated Introduction
	1	Updated Section 1.0 “Overview”
	1	Updated Section 1.1 “BMC Systems Roles and Responsibilities”
	1	Updated Section 1.2.1 “Trusted Internet Connection (TIC)”
	1	Updated Section 1.2.2 “Cellular Connection”

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	1	Updated Section 1.2.3 “Government Furnished Equipment”
	1	Updated Section 1.2.4 “BMC Systems Device Whitelisting Process”
	1	Updated Section 1.3.2 “Background Investigations”
	1	Updated Section 1.4 “BMC Systems Device, Appliance and Software Security Assessment Process”
	1	Updated Section 1.4.1 “GSA IT Security Scanning Process”
	1	Updated Section 1.4.1.1 “Step 1: Pre-Assessment”
	1	Updated Section 1.4.1.2 “Step 2: Induction”
	1	Updated Section 1.4.1.3 “Step 3: Assessment”
	1	Updated Section 1.4.1.4 “Step 4: Initial SAR Issuance”
	1	Updated Section 1.4.1.5 “Step 5: Vendor Remediation/SAR Issuance”
	1	Updated Section 1.4.1.6 “Step 6: BMC Systems Service and Support”
	1	Updated Section 1.4.2 “Wireless Assessments”
	1	Updated Section 1.4.3 “Encryption”
	1	Updated Section 1.4.4 “Non-Standard Software Review Process (BSN Consoles)”
	1	Added Section 1.4.5 “Variable Refrigerant Flow (VRF) in HVAC Controls”
	1	Updated Section 1.5 “Building Systems Network (BSN)”
	1	Removed Previous Section 1.5.1 “What is the Building Systems Network (BSN)?”

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	1	Moved and Updated Section 1.5.1 “BSN Operations and Maintenance Roles and Responsibilities”
	1	Moved and Updated Section 1.5.2 “BSN Evolvement and Implementation”
	1	Added Section 1.5.2.1 “History of BSN”
	1	Moved and Updated Section 1.5.2.2 “Current Implementation of BSN (TrustSec and Microsegmentation)”
	1	Removed Section 1.5.3.1 “BSN I: ACLs and Dedicated VLANs”
	1	Removed Section 1.5.3.2 “BSN II: Dynamic Multipoint Virtual Private Network (DMVPN)”
	1	Removed Section 1.5.3.3 “BSN III: Software-Defined Wide Area Network (SD-WAN)”
	1	Removed Previous Section 1.5.4 “Expected Changes Once the BSN ACL is Applied”
	1	Removed Previous Section 1.5.5 “How to Access Virtual Servers in the BSN”
	1	Removed Section 1.5.6 “BSN Consoles”
	1	Removed Section 1.5.6.1 “How to Obtain a BSN Console”
	1	Removed Section 1.5.6.2 “How to Access BSN Consoles”
	1	Removed Section 1.5.6.3 “Installing Software on the BSN Console”
	1	Moved and Updated Section 1.5.3 “Standard BSN Configurations”
	1	Removed Section 1.5.8 “Using Citrix VDI and BSN Consoles”
	1	Moved and Updated Previous Section 1.5.4 “Steps to Integrate Sites onto the BSN”

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	1	Removed Previous Section 1.5.9.1 “Preparation”
	1	Removed Previous Section 1.5.9.2 “BSN Preparation Meeting and Training”
	1	Removed Previous Section 1.5.9.3 “Citrix VDI Access and Use”
	1	Removed Previous Section 1.5.9.4 “Migration”
	1	Updated Section 1.6 “Incident Response (IR) and Building Recovery (BR) Exercises”
	1	Updated Section 1.6.1 “Incident Response”
	1	Updated Section 1.6.2 “Building Recovery Exercises”
	2	Updated Section 2.0 “Overview”
	2	Updated Section 2.1 “Network Roles and Responsibilities”
	2	Removed Previous Section 2.2 “GSA Network and Uptime”
	2	Moved and Updated Section 2.2 “Standards for Interoperability”
	2	Moved and Updated Section 2.3 “Network Topology”
	2	Moved and Updated Section 2.3.1 “Network Design Requirements”
	2	Added Section 2.4 “Requesting and Installing a GSA Circuit”
	2	Added Section 2.4.1 “How to Locate a Demarc Room and Demarc Extension Room”
	2	Updated and Moved Section 2.4.2 “How to Request a GSA Circuit and the Installation Process”
	2	Moved and Updated Section 2.4.3 “Important Considerations in the Circuit Installation Process”

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	2	Moved and Updated Section 2.5.1 “Requesting and Installing Switches”
	2	Moved and Updated Section 2.5.2 “Installing and Connecting Hardware”
	2	Removed Section 2.5.4 “Acceptance of Non-Standard Hardware”
	2	Added Section 2.5.2.1 “Types of Connections Allowed”
	2	Added Section 2.5.2.2 “Alternate Connectivity Options for Approved BMC Devices”
	2	Updated Section 2.6 “BACnet”
	2	Updated Section 2.6.3 “Implementing BACnet on a Wide Area Network (WAN)”
	2	Updated 2.6.3.1 “UDP Port Assignment”
	2	Updated 2.6.3.3 “Using a BACnet Broadcast Management Device (BBMD)”
	3	Updated Section 3.0 “Overview”
	3	Moved and Updated Section 3.1 “Cabling Roles and Responsibilities”
	3	Moved and Updated Section 3.2 “Cabling Infrastructure Standards”
	3	Moved and Updated Section 3.2.1 “Minimum Requirement for Ethernet Cabling”
	3	Removed Previous Section 3.2.2 “General Architecture”
	3	Moved and Updated Section 3.2.2 “Attenuation Limit”
	3	Removed Previous Section 3.2.3 “Cabling Installation Options”
	3	Moved and Updated Section 3.2.3 “How are GSA IT Cabling Standards Enforced?”

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	3	Removed Section 3.2.4 “Cabling Installation Support”
	3	Removed Previous Section 3.3 “Data Circuit Installation”
	3	Moved and Updated Section 3.3 “Cabling Installation”
	3	Removed Previous Section 3.3.1 “Data Circuit Installation Roles and Responsibilities”
	3	Removed Previous Section 3.3.2 “Process for Data Circuit Requests and Sites Visits”
	3	Removed Previous Section 3.3.3 “Important Considerations in the Data Installation Process”
	4	Updated Section 4.1 “BMC Systems Server Roles and Responsibilities”
	4	Updated Section 4.2.1 “Why Go Virtual?”
	4	Removed Section 4.2.4 “Server Security Hardening”
	4	Updated Section 4.3.1 “Step 1: Submit Server Request Form”
	4	Updated Section 4.3.2 “Step 2: Schedule Server Solutions Meeting with TechOps”
	4	Updated Section 4.3.3 “Step 3: Server Deployment Process”
	4	Moved and Updated Section 4.3.4 “Do’s and Don’ts for Application Installations”
	4	Removed Previous Section 4.4 “Application Installation and Maintenance Guidelines”
	4	Moved and Updated Section 4.4 “Application Access”
	4	Removed Previous Section 4.4.1 “Installation and Maintenance Roles and Responsibilities”
	4	Added Section 4.4.1 “How to Request Different Types of Access”

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	4	Moved and Updated Section 4.4.2.2 “How to Access a Web Application via Citrix VDI”
	4	Removed Previous Section 4.4.3 “Temporary Server Administrator Access Requests and Reboots”
	4	Moved and Updated Section 4.4.3.1 “How to RDP to a Server via Citrix VDI”
	4	Removed Previous Section 4.4.4 “Approval Authority Table”
	4	Removed Previous Section 4.4.5 “Dedicated Server Support During Installation”
	4	Removed Previous Section 4.4.6 “Copying Files to a Server on the BSN”
	4	Removed Previous Section 4.4.7 “Simple Mail Transfer Protocol (SMTP) Email Server Information”
	4	Moved Section 4.5 “Server Maintenance and Support”
	4	Moved Section 4.5.1 “Server Monitoring and Backup”
	4	Moved Section 4.5.2 “Server Patching”
	4	Removed Previous Section 4.5.2.1 “How to Request RDP Access to a Server”
	4	Moved and Updated Section 4.5.2.1 “Communications for BMC Systems Contacts”
	4	Moved and Updated Section 4.5.2.2 “Planned Maintenance and Outages”
	4	Moved and Updated Section 4.5.2.3 “Unplanned Maintenance and Outages”
	5	Added Chapter 5 “BSN Consoles”
	6	Moved Previous Chapter 5 to Chapter 6

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	6	Updated Section 6.0 “Overview”
	6	Updated Section 6.1 “Technical Support Roles and Responsibilities”
	6	Moved Section 6.2 “Initial Troubleshooting Steps”
	6	Added Section 6.3 “Reporting a BMC Systems Issue”
	6	Moved and Updated Section 6.4 “BMC Systems Support Workflow”
	6	Moved and Updated Section 6.4.1 “BMC Systems Application Issue”
	6	Added Section 6.4.2 “BMC Systems Hardware”
	6	Moved and Updated Section 6.4.3 “Network Issue”
	6	Moved and Updated Section 6.4.4 “BMC Server Issue”
	6	Moved and Updated Section 6.4.5 “BSN Console Issue”
	7	Moved Previous Chapter 6 to Chapter 7
	7	Updated Section 7.0 “Overview”
	7	Updated Section 7.1 “Advanced Metering System Roles and Responsibilities”
	7	Updated Section 7.2 “Advanced Metering System Architecture”
	7	Updated Section 7.3 “Standards for Interoperability”
	7	Updated Section 7.4 “New Installations”
	7	Moved and Updated Section 7.4.1 “Sample Network Diagram”
	7	Added Section 7.4.2 “Cabling”

DocuSign Envelope ID: 2CD901F9-8EC1-44A0-BAA0-D74ECC705514

	7	Moved and Updated Section 7.5 “Technical Support for AMS”
	7	Moved and Updated Section 7.5.1 “Support Form”
	7	Moved and Updated Section 7.5.2 “Troubleshooting Process”
	8	Moved Previous Chapter 7 to Chapter 8
	8	Updated Section 8.0 “Overview”
	8	Updated Section 8.1 “Physical Access Control Systems Roles and Responsibilities”
	8	Updated Section 8.2 “Security”
	8	Updated Section 8.4 “Project Flow”
	8	Updated Section 8.5 “GSA IT EPACS Support”
	9	Moved Previous Chapter 8 to Chapter 9
	9	Added Section 9.1 “Contract Language IT Security Requirements”
	9	Updated Section 9.2 “Scope of Work Template (BAS Hardware/Software Upgrades)”
	10	Moved Previous Chapter 9 to Chapter 10
	10	Updated Section 10.0 “Overview”
	10	Updated Section 10.1 “Tips for Running a Successful BMC Systems Project”