Building Technologies Technical Reference Guide

Version 2.0

REDACTED - FOR EXTERNAL DISTRIBUTION

June 11, 2021

Approvals

DocuSigned by:
Phil Klokis
6F8E4CB418E2409...

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

DocuSigned by:
Bo Berlas
FD7470264B1544F...

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

DocuSigned by:
Andrew Heller
AC382BA5365B4B2...

Andrew Heller
Assistant Commissioner
Public Buildings Service: Office of Facilities Management

DocuSigned by:
Andrew N Young
2747A662FDFD490...

Andrew Young
Assistant Commissioner
Public Buildings Service: Office of Design and Construction

DocuSigned by:
Robert Carter
CCAF8EC6648D94A2...

Robert Carter
Associate Administrator
Office of Mission Assurance

Table of Contents

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 be 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 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
- Office of Mission Assurance (OMA)
- Office of Design Construction (ODC)

The Building Technologies Technical Reference Guidelines (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 its 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, physical access control systems (PACS), renewable energy systems, and digital signage. 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 BMC System Technology Policy. For guidance on smart building implementations and industry best practices for building automation systems, please refer to:

- [redacted]
- [redacted]
- [redacted]

Revision History

Version	Date
Version 1.0	June 2011
Version 1.1	February 2014
Version 1.2	September 2016
Version 2.0	June 2021

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

Chapter 1

Policy/Standards and IT Security

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 devices/systems. 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 projects in preparing for assessment and authorization activities required for building systems projects.

Current policies for assessment and authorization of systems and devices on the Building Systems Network are based on the *National Institute of Standards, and Technology (NIST) Special Publication (SP), 800-53 rev4, Security and Privacy Controls for Federal Information Systems and Organizations*. The Building Systems Network (BSN) servers supporting the building automation systems, and associated devices, have been issued a Federal Information Security Modernization Act (FISMA) Moderate Authority to Operate (ATO). Additionally, the GSA-IT Security team has issued guidance and procedure documents on the assessment process that detail the required steps for security assessments, roles and responsibilities, along with the SLAs/time frames for evaluation. These reference documents can be found on [redacted]

1.1 BMC Systems Roles and Responsibilities

- **GSA-IT Network Operations and Management (Network Team):** The network team is responsible for the entire IP transport layer to include all routing and switching equipment and access to IP connectivity. They have command responsibility for the GSA Local Area Network (LAN) and GSA Wide Area Network (WAN). The Network Team is the sole provider for IP/subnet allocation at the building level as well as management of network devices (switches and routers), on the GSA network. They are also responsible for managing the BSN's connectivity to the rest of the network. ***Please Note: PBS is responsible for the controllers/devices. GSA-IT provides connectivity up to the switch port, on the network.***

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

- **GSA-IT Security Operations Team (SecOps):** SecOps is responsible for operating the GSA cybersecurity stack that provides security services to PBS. The security services include, but are not limited to, endpoint protection, perimeter defense, vulnerability scanning, enterprise logging, and analysis. GSA-IT Security performs regular scans of BSN servers as part of compliance validation. SecOps is also responsible for facilitating aspects of authorization control including authoring the Assessment and Accreditation (A&A) documents, performing risk assessments, managing the system compliance over the life of the ATO and managing the Plan of Action and Milestones (POA&M) items specific to the Building Technologies systems.

- **GSA-IT Security BMC Device Assessment Team (BMC Lab):** The BMC Device Assessment Team performs hardware/firmware/software assessments on devices designated as BMC components. They are also responsible for reporting the proper configuration of the device on any GSA network 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 Device and Application Security Assessment Process.***

- **BSN Information System Security Manager (ISSM) and Information System Security Officer (ISSO):** The BSN ISSM, and ISSO are responsible for facilitating aspects of authorization control including authorizing the A&A documents, performing risk assessments, managing the system compliance over the life of the Authority to Operate (ATO), and managing the POA&M items specific to the BSN.

- **Regional PBS Project Teams:** This includes Regional Smart Building Team members, BAS specialists, contracting officers, project managers, facility managers, etc. They are responsible for ensuring that any BMC-IT systems contracted, purchased, owned and/or operated in the regions adhere to Policy and Implementation guidance within this document and other applicable GSA guides. Also, these teams are to articulate any contractual agreement with the information technology vendor who provides products and/or services to PBS, including hardware, software and Service Level Agreements. **Additionally, the regions are responsible for contacting the Buildings Technology Services Division (BTSD) prior to the award for applicable contract and implementation requirements. They are responsible for the installation, configuration, and management of the application software.** In addition, they are to complete the Application Documentation Form for TechOps in a timely manner in order to ensure monitoring and backup routines are established. ***Please Note: See Chapter 4 for links to required documents.***

- **Vendor/Contractor:** Responsible for adherence to GSA-IT policies, ensuring BMC devices and applications are secure, meet Security Assessment Report (SAR) provisions, completing documentation related to the security and support of their application and devices, and for providing maintenance/support of their devices and software. Vendor/contractor must meet all provisions of the latest remediated Security Assessment Report for any software and/or hardware connected to the GSA network or BSN LAN extension.

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.

2100.1L CIO CHGE 1 GSA Information Technology (IT) Security Policy states:

"All network devices that are either owned, managed, connected to a GSA facility, and/or handle 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 the GSA to provide the following security functions for any devices connected to the GSA networks:

- Monitoring, incident response, vulnerability assessment, vulnerability management, incident reporting, engineering support, and the enforcement of the agency's specific security policy at the hosted facility.

- Trained, qualified, and cleared staff to support security functions 24x7.

- Limited inbound and outbound connections so that only necessary services are allowed.

- Centralized, secured, and unified management of security events in order to protect the integrity of the U.S. Government data and its infrastructure.

Please Note: At no time should a GSA hosted BMC system(s) be made accessible to the public internet or via any third-party network connection, referred to as "rogue circuits". All network traffic must transit through a TIC, which is a network circuit that is managed by GSA-IT. Any use of 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

GSA prefers all BMC devices be connected to the GSA building systems network. GSA realizes that under certain circumstances, connecting BMC 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 devices utilizing cellular transport must successfully complete the GSA 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.

1.2.3 Government Furnished Equipment

Federal Acquisition Regulation (FAR) 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 provided for facility managers, associated with BMC Systems. Vendor provided computer hardware is not allowed to connect to the GSA network and can only be used for pre-commissioning purposes (at no point can it access the GSA network). If vendor-provided devices, workstations or servers are discovered, they are subject to removal without warning. Alternatively, Citrix-VDI can be used as an alternative to GFE, when applicable. ***Please Note: See Chapter 4 for details.***

- **Network Equipment:** This includes, but is not limited to, any equipment that provides networking capabilities, i.e., hubs, wireless access points, switches, and routers.

- **Computer Hardware**: This includes, but is not limited to servers, printers, smart devices, computers, laptops and their peripherals (monitors, mice and keyboards).

As buildings are integrated with the GSA network, GSA-IT will make every effort to provide up to two laptops to these sites. The purpose of the laptop is to provide building management staff with access to their BMC system application interfaces.

Please Note: Availability of hardware is dependent on the availability of funding dedicated for this purpose, which may or may not be renewed on an annual basis. Existing GSA workstation refreshes will still be coordinated through the regional GSA-IT manager's office. No hardware (workstations, servers, switches, etc.) will be provided unless an approved network diagram is submitted. See Section 2.4 for details about network diagram requirements and submission.

1.2.4 BMC Device Whitelisting Process

Cisco Identity Services Engine (ISE) is a next-generation, identity and access-control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. ISE 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 needs to 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 Device and Application Security Assessment Process.*** Once the device is reviewed and remediated, the BTSD Technical PM will need support from PBS and the project team to prepare an updated network riser diagram, (which lists all devices, their IP addresses, MAC addresses, and location) to the network team. Once documentation has been updated, the BTSD Technical PM submits a "MAB" or an ISE exception ticket in Service Now, in order to whitelist the devices.

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 Homeland Security Presidential Directive-12 (HSPD-12) 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

In August 2004, President George W. Bush signed the Homeland Security Presidential Directive-12 (HSPD-12) which 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 [redacted] site for details on how to initiate the credentialing process.

1.3.2 Background Investigations

The mandatory minimum background investigation level for access to any GSA system is the preliminary adjudication of Tier 1. However, Per *GSA CIO Policy 2100.1*, 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

All access to GSA information systems must comply with the requirements of *GSA Information Security Policy 2100.1L*. 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 Device and Application Security Assessment Process

Before any IP-addressable hardware, software or IT device/system can be connected to the GSA network, GSA-IT will need to assess and approve the solution and all identified vulnerabilities must either have been remediated or have an Acceptance of Risk (AOR) by GSA-IT's Authorizing Authority.
Please Note: Scans are authenticated and have a process in place to securely pass authentication data. This ensures that the systems which touch the GSA network have the proper controls implemented in accordance with security requirements.

A Security Assessment Report (SAR) is produced by GSA-IT Security once the device has been assessed, which is provided to the PBS stakeholders and the vendor. The assessment report allows the GSA to understand and accept the risk to agency operations, agency assets, or individuals, based on the implementation of an agreed upon set of security controls. The contractor/vendor is responsible for mitigating all security risks identified in the SAR. Vulnerabilities must be mitigated within the appropriate timeframe as described in the SAR mitigation plan along with milestones and timelines for remediation for consideration of GSA-IT in order to connect to the GSA network.
GSA-IT Security only needs to assess a certain model of a device the first time it is introduced to the GSA network. Once a device has completed the remediation process and has a remediation/hardening plan in place, all other projects can use that SAR to configure the device accordingly. This procedure is repeated on a three-year (maximum) cycle or until a major version change has been implemented by the manufacturer. As items get evaluated and receive favorable concurrence by the IT Security Team, they will be added to the [redacted] which is the backend for the [redacted] ***Please Note: Both links have restricted access within the GSA firewall.***

PBS stakeholders can find the most current list of devices that are either being assessed or have been assessed in the past and are approved to be used in either of those links. The list is not to be used either for inclusion or exclusion of listed components and is only provided as a guide to devices that have completed favorable assessments and are deemed as "remediated". ***Please Note: GSA-IT Security will need to evaluate non-IP wireless devices due to the higher level of threat posed by wireless devices. See Section 1.4.2 for more details.*** Any device that is not approved or has an expired SAR will risk losing the Authority to Operate (ATO).

More information regarding the assessment process can be found in *BAS Security Assessment Process [CIO IT Security 16-76]* which is located under IT Security Procedural Guides on GSA[redacted]

1.4.1 GSA-IT Security Scanning Process

In order to request a scan, the hardware or software being proposed must be under contract for a current project. ***Please Note: GSA does not pre-scan/pre-assess hardware/software from vendors.*** To begin the process, an [redacted] (ARF) must be completed, before the device is shipped to the BMC Assessment Team . 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 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 Assessment Team. Alternatively, the documentation can be emailed directly to [redacted]

The BMC security assessment process is broken down into six steps: Pre-assessment, Assessment Induction, BMC Assessment, SAR Issuance, BMC Vendor Remediation, and BMC Post-Assessment.

1.4.1.1 Step 1: BMC Pre-Assessment

The BTSD is responsible for working with BMC Vendors to identify BMC solutions needing assessment. During this stage, the BTSD will collaborate with the BMC Vendor to coordinate and submit the pre-assessment requirements. The requirements include electrical specifications, documentation requirements, technical prerequisites, and submitting the required forms. The BMC Assessment Team is responsible for reviewing documentation and technical specifications to identify compliance with minimum security requirements and accepting or rejecting the BMC solution into the BMC Assessment Lab.

The device should be sent to the BMC lab configured and hardened as it will be installed on the GSA network (unnecessary ports and services closed, etc.). The device should also arrive properly assembled for power. The BMC 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 lab and configure appropriately).

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.)
  - 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 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 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

- 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 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 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
    - Configured HTTPS to be enabled and HTTP disabled
    - Be configured with FIPS 140 Compliance (if possible)
- 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
    - 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 (except Windows CE) or UNIX/Linux based operating system,

antivirus software must be installed, and a plan must be in place for keeping the software updated

- Disable protocols such as Telnet, SSH, TFTP and FTP

- Disable wireless communications unless previously specified as required (802.11 Wi-Fi, Bluetooth, ZigBee, Z-Wave, UHF/RHF, etc.)

Please Note: Any configuration required by IT Security or lack of documentation may result in delaying the security evaluation 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: BMC Device and Supervisory Control Software (SCS) Induction

The BMC Assessment Team will attempt to power on the BMC Device, access the device, and establish network connectivity. The BMC Assessment Team will make a reasonable attempt to work with the vendor during this process. If, after ten business days, the assessor is unable to access the device or establish network connectivity, the priority will be moved to the bottom of the queue until the issues are corrected. If the device is not corrected within 20 business days, it will be removed from the prioritization sheet and the BMC Assessment team has the right to reject the device and close the assessment ticket. The BMC Smartsheet page will be updated to identify the configuration deficiency and the assessment will be closed. At this point, the device will be shipped back to the vendor within five business days. The vendor will be notified and provided the shipping tracking number.

An SCS is considered inducted once all the following have been completed:

- A server has been reserved

- An image build has been completed by TechOps

- All installation files are available

- An installation meeting has been scheduled.

During this phase, the BMC Vendor will be utilized to assist the BMC Assessor in properly installing and configuring the SCS. An activation license is required prior to the installation meeting.

1.4.1.3 Step 3: BMC Assessment

The BMC Assessment process utilizes a systematic, repeatable approach to uniformly evaluate every type of system, whether physical access controls, building automation, specific applications, or wireless technology. The assessment process consists of several types of reviews in order to test all aspects of a solution. The sections below provide additional detail on each assessment step. The SLA response time will not start until the device is accepted into the BMC Assessment Lab or the software is successfully installed. The SLA timetable does not include the time to mitigate issues or troubleshoot problems with the BMC vendor. The BMC Smartsheet page will be updated to reflect the status of each assessment item noted below.

Top Ten Most Common Vulnerabilities in BMC Systems Assessments:

- **Cross-Site Scripting:** This could result in impacts such as a hijacked account, information theft, browser redirection or denial of service.

- **Mitigation:** Cross-Site Scripting attacks can be avoided by carefully validating all input, and properly encoding all output. Implement validation globally using standard ASP.NET Validation controls, or directly in system coding

- **Insufficient Documentation:** Documentation available for the device does not provide administration instructions or complete information on the inbound and outbound communications of the device.
  - **Mitigation:** GSA-IT requires that, "Documentation must be obtained or created to describe how security mechanisms are implemented and configured within the IT system." Obtain documentation sufficient to install, configure, administer, and monitor devices.

- **Least Privilege**: Documentation available for the device does not provide required configuration settings to enforce least privilege compliance.
  - **Mitigation:** Information systems must be configured to the most restrictive mode consistent with operational requirements and in accordance with appropriate procedural guides from NIST and/or the GSA to the greatest extent possible. Implemented configuration settings should be documented and enforced in all subsystems of the information system." Obtain documentation sufficient to securely configure these devices.

- **Configuration Management:** Documentation available for the device does not provide a configuration management plan.
  - **Mitigation:** A system configuration management plan must be developed, implemented, and maintained for every IT system managed by the GSA, to ensure changes are authorized, tracked and validated.

- **Insufficient Auditing**: No evidence is provided that the device is auditing to GSA required level of detail.
  - **Mitigation**: The GSA requires security activity auditing capabilities to be employed on all GSA information systems and that audit logs are in compliance with GSA auditing requirements.

- **Unencrypted Login Form**: An attacker who exploited this design vulnerability would be able to utilize the information to escalate their method of attack, possibly leading to impersonation of a legitimate user, the theft of proprietary data, or execution of actions not intended by the application developers.
  - **Mitigation**: Sensitive areas of web application must have proper encryption protocols in place to prevent login information and other data that could be helpful to an attacker from being intercepted. Per GSA policy, Web sites (internal and public) with logon functions, must implement TLS encryption with a FIPS 140-3 validated encryption module.

- **Logins Sent Over Unencrypted Connection**: An attacker who exploited this design vulnerability would be able to utilize the information to escalate their method of attack, possibly leading to impersonation of a legitimate user, the theft of proprietary data, or execution of actions not intended by the application developers.
  - **Mitigation:** Sensitive areas of web application must have proper encryption protocols in place to prevent login information and other data that could be helpful to an attacker from being intercepted. Per GSA policy, Web sites (internal and public) with logon functions, must implement TLS encryption with a FIPS 140-3 validated encryption module.

- **No Encryption**: Sensitive information is transmitted without protection.
  - **Mitigation:** Sensitive areas of web application must have proper encryption protocols in place to prevent login information and other data that could be helpful to an attacker from being intercepted. Per GSA policy, Web sites (internal and public) with logon functions, must implement TLS

encryption with a FIPS 140-3 validated encryption module.

- **Unnecessary Services**: Services were available with no documented need for their use.
    - **Mitigation:** Disable all unnecessary services. Document all necessary services. Unnecessary services provide malicious users additional vectors to perform an attack.
- **Unnecessary Ports Open**: Insufficient or no documentation available to justify need for use of open ports.
    - **Mitigation:** Unnecessary ports provide malicious users additional vectors to perform an attack. All unnecessary ports must be closed, and proper documentation is required for necessary ports that need to remain open.

1.4.1.4 Step 4: BMC Solution SAR Issuance

Upon completion of the BMC Solution Security Assessment, the BMC Assessment Team will document all findings and vulnerabilities in a SAR. The SAR provides a discussion of the security assessments results which details the numerical identifier, finding name, description, associated NIST SP 800-53 controls, any GSA policy reference, and a recommended fix. The SAR will be utilized within the remediation phase to provide vulnerability tracking and responses pertaining to the remediation effort. The SAR will also include the scan reports and the manual assessment checklist that was completed during the assessment process. Updates to the associated SAR creation and issuance date will be provided by the BMC Assessment Team on the BMC Smartsheet page.

1.4.1.5 Step 5: BMC Vendor Remediation

A BMC solution is required to go through the remediation process if the SAR is issued with open 'critical', 'high', or 'moderate' finding. The SAR remediation phase begins once the SAR is distributed to the BMC vendor and appropriate BMC stakeholders. This is a separate process from the BMC Device Assessment Phase. The GSA-IT Security team will provide guidance for remediation or mitigation of the findings. Vulnerabilities are to be remediated by fixing the identified vulnerability. If the vulnerability cannot be remediated within an acceptable timeframe, 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. The AoR can allow up to 12 months for a vulnerability to be remediated. Per *GSA Information Security Policy 2100.1L* all vulnerabilities (Critical, High or Medium) must be mitigated. AORs are not common and are approved on a case-by-case basis. If new vulnerabilities are discovered after the system has been remediated and integrated onto the network, the PBS project teams are responsible for ensuring that the proper software maintenance and contracting is in place in order to mitigate the vulnerabilities. Per GSA-IT policy, 'critical' and 'high' risk findings must be mitigated within 30 days, and 'medium' risk findings within 90 days.

It is important to note that the BMC solution SAR is a snapshot in time, whose results lose relevancy over time as new vulnerabilities and exploit techniques are identified. As such, if a BMC vendor cannot respond to the GSA with actionable remediation of the identified findings within 120 business days (six months) from the issuance of the BMC SAR, the BMC Assessment team has the right to categorize the BMC solution as non-remediated and close the Smartsheet page. The BMC vendor and BMC stakeholders will be notified of the non-remediation decision and the BMC device will be added to the non-remediated BMC device list on GSA's BTSD's Smartsheet page.

1.4.1.6 Step 6: BMC Solution Post Assessment

Once the remediation decision has been determined, the BMC assessment project is considered closed. If a BMC component is identified as non-remediated, GSA is prohibited from purchasing any additional components of that model since it is an identified risk to the GSA environment. The BMC Assessment Team

will review the implementation of a patch management and continuous monitoring plan during the manual assessment process.

It is the responsibility of the PBS Business Line to ensure an Operations and Maintenance (O&M) 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 an identified security incident, there may be a need to reassess the device/SCS. This section provides additional guidance for requirements as to when a re-assessment must be completed.

1.4.2 Wireless Assessments

Wireless technologies must have a minimum of AES 128 encrypted level, ideally 256-bit AES encryption. All wireless solutions must adhere to the "2100.2B CIO P GSA Wireless Local Area Network (LAN) Security" guide before they can be connected to the GSA network. This guide mainly covers devices operating 802.11. 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, such as 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) and low-level frequency without protection, such as Global System for Mobile Communications (GSM) Band and Code Division Multiple Access (CDMA) (3G/4G/LTE/5G).

The requirements for each technology are:

- **802.11 Requirements:** All new GSA wireless LAN implementations must meet 802.11i requirements for encryption using the Counter Mode with CBC-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).
- **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 Layer is 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).

1.4.3 Encryption

The Federal Information Processing Standard (FIPS) 140-3 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 140-3 compliant protocols, as well as machine-to-machine transfers.

1.4.4 Non-Standard Software Review Process (BSN Servers/Consoles)

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, which focuses on ensuring software are currently supported, are generally secure and free of vulnerabilities. This process is managed by the Technical Standards Committee (TSC), within the Office of the Chief Technology Officer (CTO). TSC gathers input from Legal, 508 Compliance, and IT Security to decide on whether the software is approved for expanded use at the GSA. During the review process, the software requester may be contacted with additional business questions. Typical questions include: "How many people will use the software", "What are the initial and recurring costs", and "Whether any approved alternatives were considered".

To start the evaluation process, submit a catalogue request in ServiceNow. Please be sure to keep the BTSD Technical PM included in the process so that they can ensure it goes through the appropriate reviews. Additional information pertaining to the evaluation process can be found here [redacted] Projects need to ensure that only approved software is installed on GFEs, including the BSN consoles.

If there is a need to install non-standard software on a BSN console, discuss the application need with the regional BTSD Technical PM. The software must complete the TSC evaluation process before it can be installed. Once that approval has been received, contact the regional BTSD Technical PM/RBITS to receive administrative rights on the BSN console in order to initiate software install.

The software approval process also applies to BMC server applications. Once the server software has been reviewed and remediated by IT Security, projects can request temporary administrative rights to their servers, in order to install the application.

1.5 Building Systems Network (BSN)

As this chapter describes, there are Federal and GSA-specific IT security policies and standards that apply to the purchase and/or use of all IT-related products and services. Any piece of hardware or software that does not meet these standards is thereby introducing a level of risk through the ownership and/or use of that system or component. Particularly, those devices that are enabled for IP-based network communication are treated with the most caution, as they can impact and be impacted by other IP-based systems, which are the most prevalent types of systems associated with GSA's IT environment. Wireless based devices, or components with other capabilities deemed to introduce risk, are also subject to review by the GSA's IT SecOps and IT Security Engineering organizations.

The scanning and evaluation program outlined in this chapter is designed to identify potential vulnerabilities

with any IP-based device that is being proposed for integration to the GSA network, to include the categorization of the risk associated with those vulnerabilities. Other non-IP devices may require evaluation by GSA-IT Security, based on the capabilities of that device and any perceived risk that it introduces. As defined in the scanning and evaluation process, the SAR is reviewed with the manufacturer or responsible vendor to have them remediate or mitigate findings to such a degree that the AO is willing to accept the risk and allow the hardware or software to be used on the GSA network.

The challenge associated with the various building systems technologies is that, while advances have been made in the core functionality of these devices necessary for making buildings easier to operate, increased functionality, particularly as it relates to network communication, introduces increased risks. The advanced metering, building automation, lighting control and physical access control systems industries, for example, have not positioned themselves the way that most other IT products companies have, with a focus on IT security. This gap in security is proving to be one that cannot be readily closed by companies in these industries and within a timeframe that aligns with contractual 'substantially complete' dates or other critical project milestones and deadlines. Still, in other cases where PBS sites are simply migrating their existing building systems to the GSA network, there is not a vendor with an open contract to engage in any of the improvements or risk mitigation related to their system components.

1.5.1 What is the Building Systems Network (BSN)?

Over the past several years, GSA-owned facilities have been making use of IP-enabled, building control devices to support increased capability, ease of use, remote access and data integration. An overwhelming percentage of building technologies either have critical or high security vulnerabilities that require an upgrade or have end-of-life components. All of which pose a threat to the GSA network. In order to reduce this risk, GSA-IT has iteratively architected a secure network infrastructure that has continued to mature to this day. Since 2012, GSA-IT has continued to improve the network security infrastructure of building systems in order to have a scalable, secure, and centrally managed architecture.

The BSN is a logically identified network, which makes use of the GSA's physical network, but uses an organization of Virtual Local Area Networks (VLAN), and firewalls to segment the IP communications from building control system application(s) and devices from the rest of the GSA business network (otherwise knowns as GSA ENT domain), by logically separating them. A private Class B network used for IP address assignment to building monitoring control system components, servers and workstations facilitates the use of multiple ACLs to effectively allow "whitelisted" communication to GSA services required to enable IT support of GSA-IT infrastructure within the BSN or to allow communications with approved external services for building systems.

Please Note: The BSN is NOT intended as a replacement for the ongoing remediation of building systems devices and applications. All new solutions procured for GSA facilities are required to meet the NIST and FISMA standards and require an Authority to Operate (ATO).

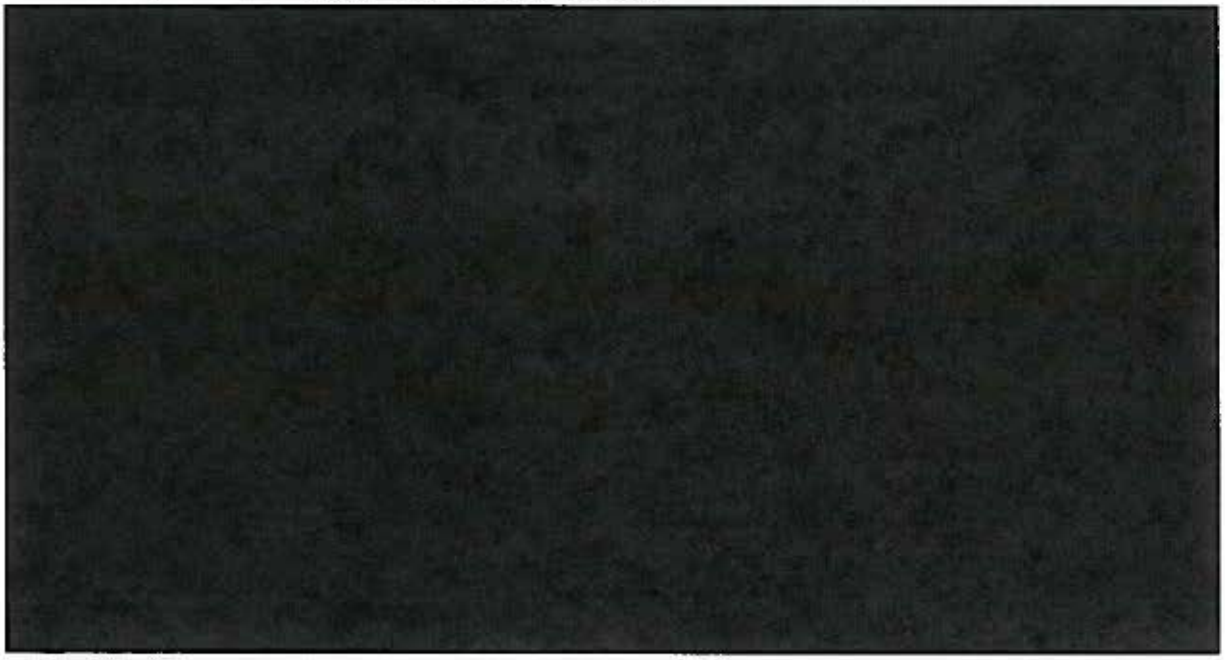
1.5.2 BSN Operations and Maintenance Roles and Responsibilities

The BSN was designed with the participation of multiple groups within GSA-IT and with cooperation from subject matter experts in the regions.

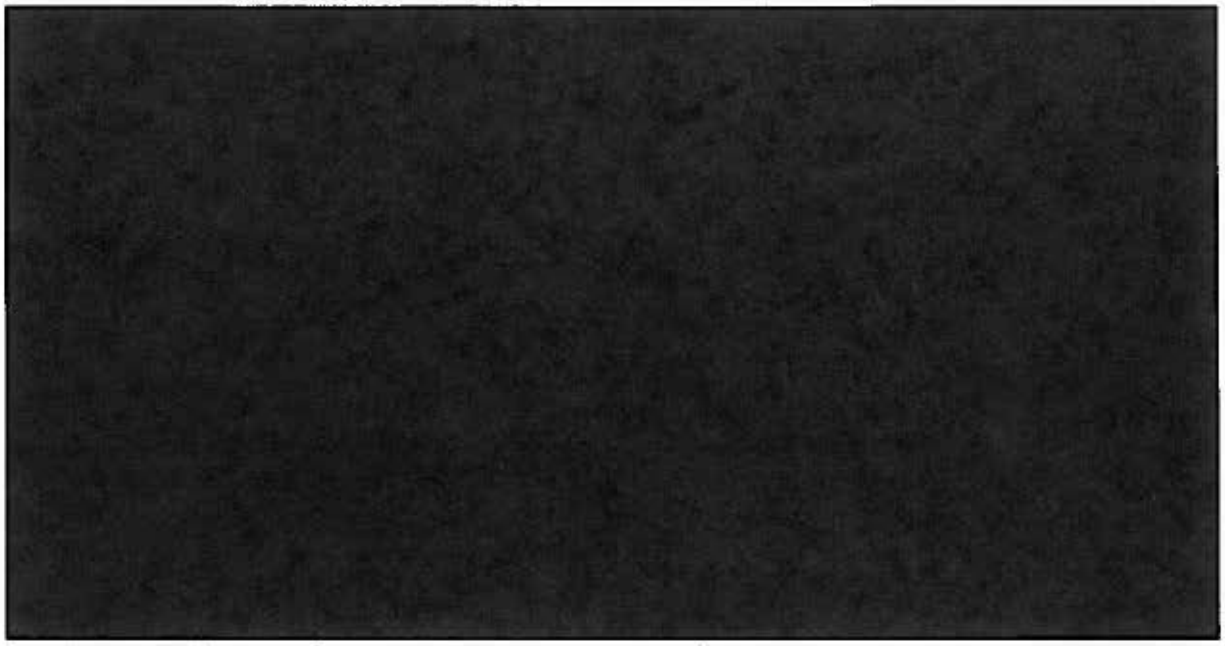
- The network management portion of the BSN is the responsibility of GSA-IT's Network team.
- The Citrix team and TechOps manage and support Citrix Virtual Desktop Infrastructure (VDI).
- Regional GSA-IT Deskside Services configures and supports workstations.
- TechOps configures and supports servers.
- The BTSD is responsible for project management in all the regions across GSA facilities.

1.5.3 BSN Evolvement and Implementation

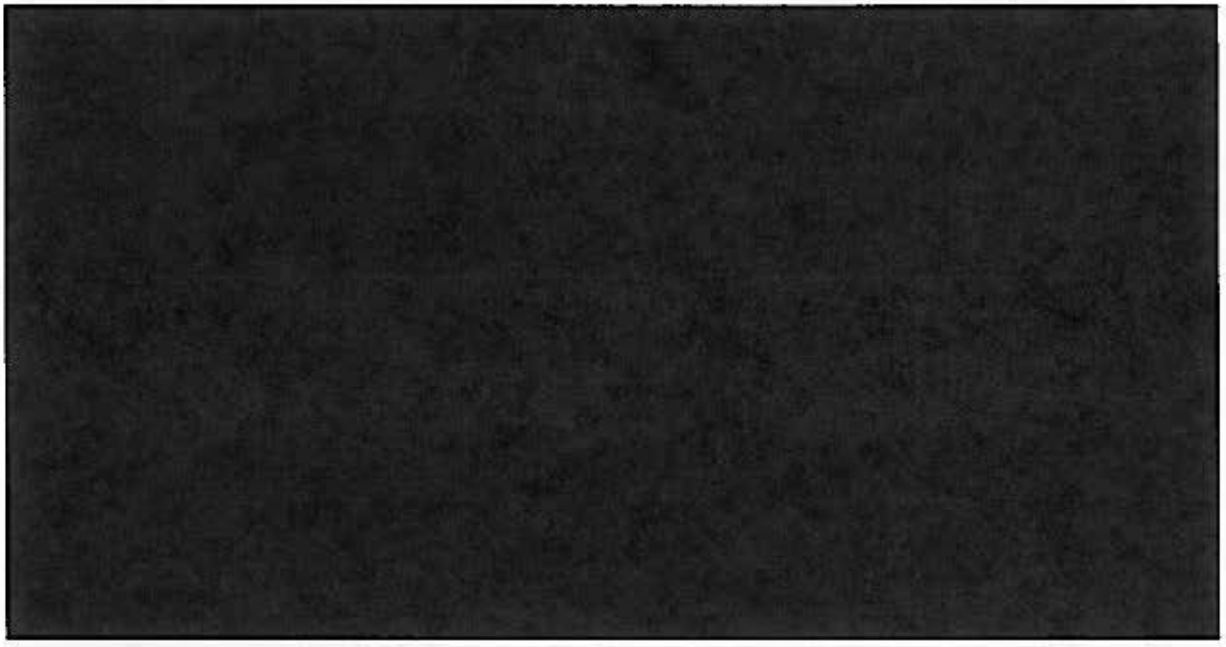
1.5.3.1 BSN I: ACLs and Dedicated VLANs



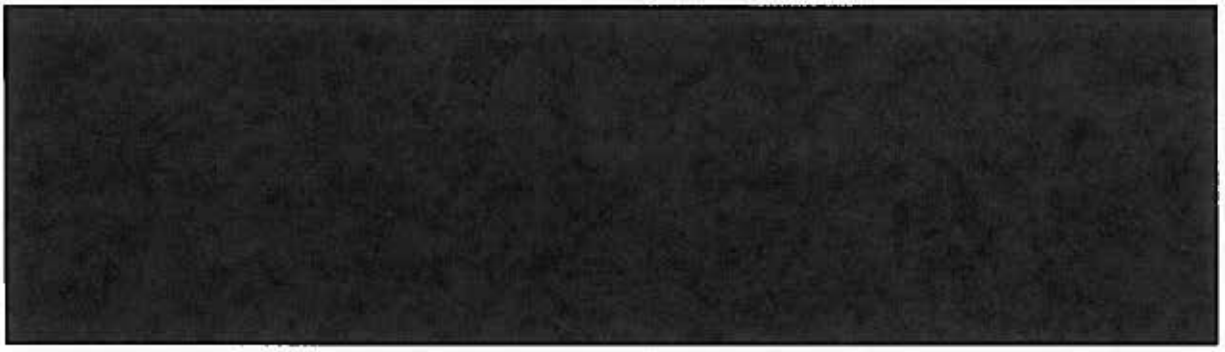
1.5.3.2 BSN II: Dynamic Multipoint Virtual Private Network (DMVPN)

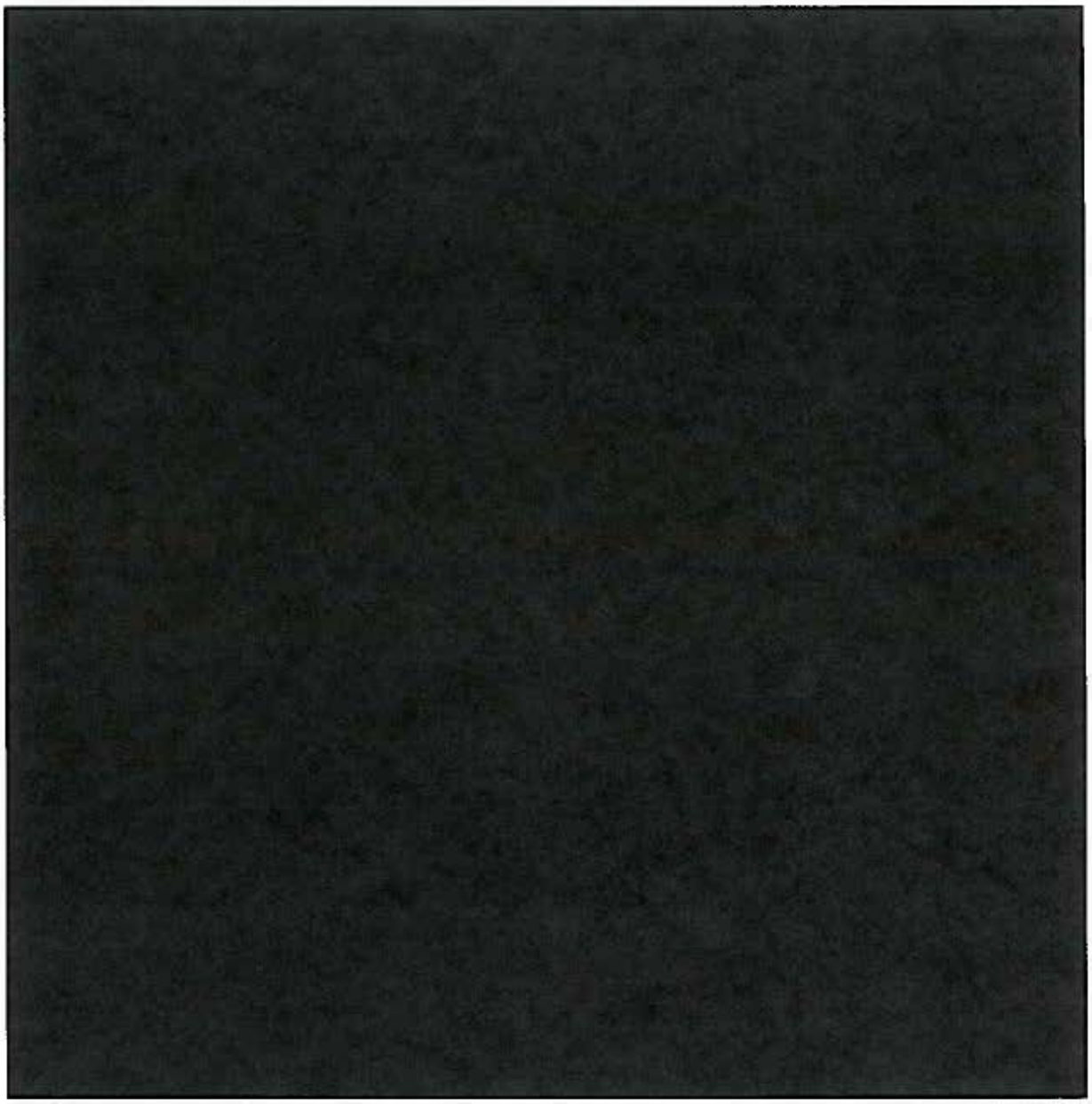


1.5.3.3. BSN III: Software-Defined Wide Area Network (SD-WAN)



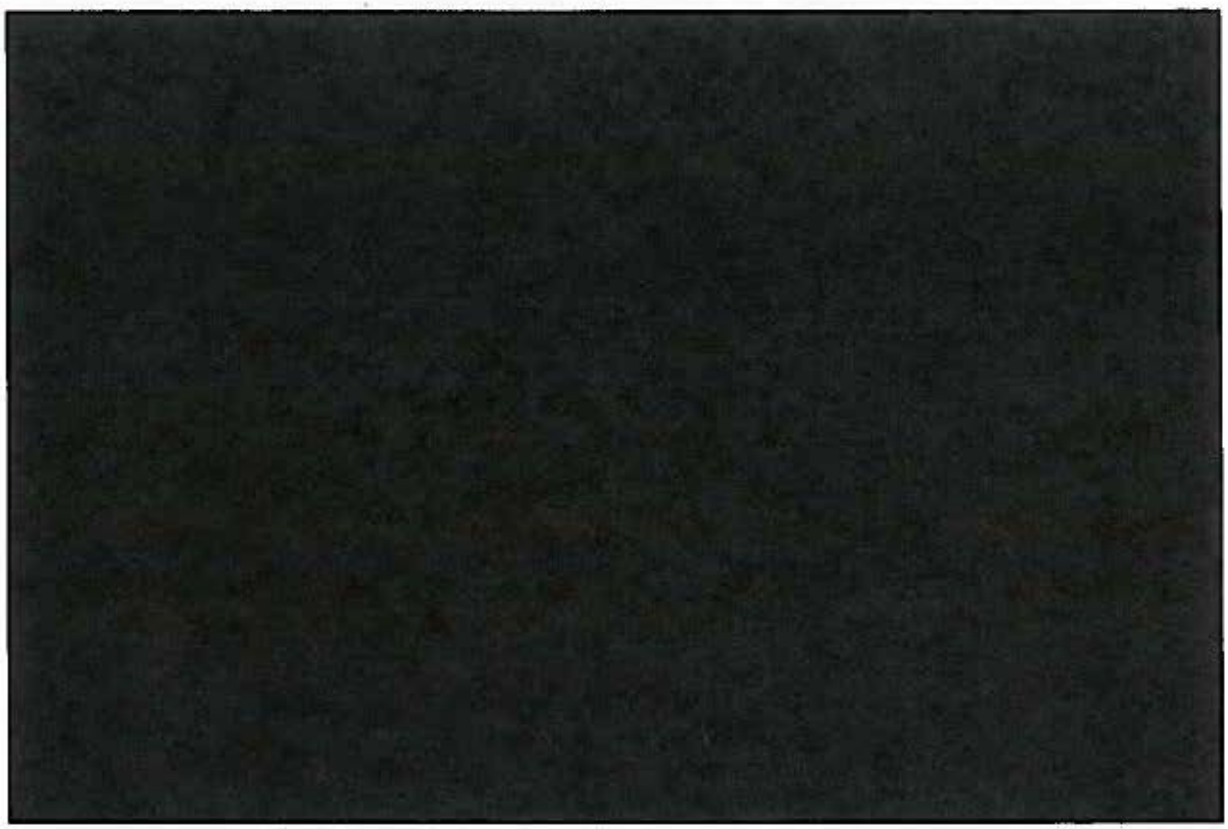
1.5.3.4 BSN IV: Trustsec and Microsegmentation





1.5.4 Expected Changes Once the BSN ACL is Applied

1.5.5 How to Access Virtual Servers in BSN



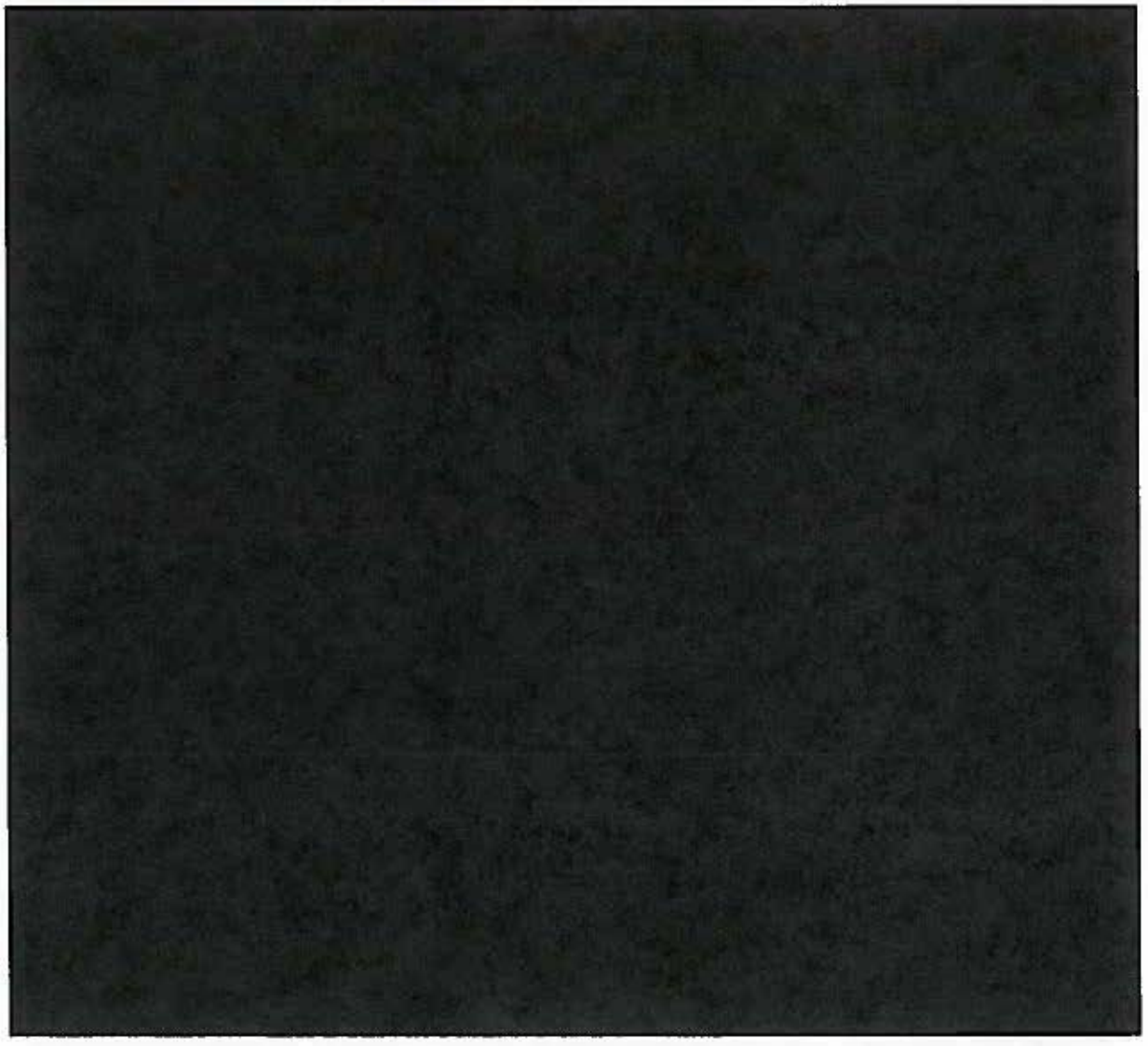
1.5.6 BSN Consoles

1.5.6.1 How to Obtain a BSN Console

1.5.6.2 How to Access BSN Consoles

1.5.6.3 Installing Software on the Building Console

1.5.7 Standard BSN Configurations



1.5.8 Using Citrix VDI and BSN Consoles

1.5.9 Steps to Integrate Sites onto the BSN from the ENT Domain

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 in order to accomplish this. All steps will be coordinated by the BTSD Technical PM.

1.5.9.1 Preparation

- Deploy a BSN console laptop to the site and ensure that it is accessible.
- Train facilities management/O&M personnel on BSN and accessing BMC systems via Citrix when accessing BMC from remote and accessing BMC systems using a BSN console within the building.
- Verify the location currently operates on a subnet compatible with BSN. Currently the ideal subnets reside on the Class B, [redacted] range. If the site does not operate on this or a compatible range then the regional BTSD Technical PM will submit an subnet request ticket within ServiceNow and indicate a new range for an existing site.
- If the site requires a new subnet range, then all equipment will need to have their IP changed to one within the new range. This will need to be coordinated with the O&M contractor and may require a subcontractor to complete the configuration change, depending on the type of equipment involved. ***Please Note: Any changes to equipment IP needs to be coordinated with building management***

and the Network Team to ensure operability before and after the change.

- BTSD Technical PM will need to request a BSN console via ServiceNow with the correct static IP and all software necessary to operate the building normally or, more importantly, during a network outage.
- For sites that were reliant on DNS, the BAS software will need to be updated to reflect the IP of devices as there is no DNS on the BSN.
- ServiceNow ticket is submitted to apply BSN ACL on date agreed by all parties

1.5.9.2 BSN Preparation Meeting/Training

Discuss the tasks necessary for migration, including roles, Citrix VDI access, how the system will be accessed post BSN cutover and migration date.

1.5.9.3 Citrix VDI Access and Use

- Create an RDP shortcut in the "BMC RDP Shortcuts" folder within Citrix VDI, if BMC application cannot be accessed via a browser.
- 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.***

1.5.9.4 Migration

- A conference call with GSA-IT, project members and facilities management, will expedite migration activities. Please work with the BTSD Technical PM to arrange a meeting with all relevant stakeholders.
- Once all the pre-migration tasks have been completed to initiate the migration, the Network Team will connect to the rest of the network.
- Once the network is connected, site personnel will need to verify they can operate their building locally on BSN console as well as access it via Citrix VDI.

1.6 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. In order 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.

1.6.1 Incident Response

Incident Response entails the contractors' ability to identify a potential cyber incident and the ability to immediately report the issue to GSA-IT [redacted] or 866-450-5250). 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. For questions about GSA's Incident Response Program, contact the GSA Incident Response Team at [redacted]

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, 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 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, reviewed and approved by regional GSA BAS government sponsors/project POCs, 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 the installing contractor, Facility Management, Operations and Maintenance (O&M) and GSA-IT and government sponsors/project POCs. The contractor shall submit their BR operational procedures in the event of a 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 preparation for internet outages.

Chapter 2

Network Infrastructure

2.0 Overview

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.

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. This is the case for the GSA and the vast majority of commercial and residential network services. Other intra-building networks, used to connect components, devices or appliances, associated with a specific system(s), such as building automation or lighting systems, use other protocols to communicate amongst the interconnected components. Wired technologies include Cat5e (if adding to existing infrastructure)/Cat6 (all new cabling, except wireless must be 6a) cables, as well as 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 closely positioned group of buildings. Whereas a Wide Area Network (WAN) covers a large geographical area such as a city, or country. A LAN has a higher rate of data transfer, 10/100/1000 Megabits per second (Mbps). GSA's WAN connects together a collection of regional and field offices along with GSA's headquarters. WAN connection speeds vary greatly and are determined by multiple factors.

The GSA WAN component is based on a combination of fiber-optic premise cabling system and Cisco router-based technology. The GSA WAN is located at all the Regional Office buildings (ROB's) and in the data centers across the country. It is also the focal point for GSA's Internet access, which includes four MPLS (6-G (500 Mbps), 7-G (500 Mbps), 11-G (1000 Mbps), 13-G (1000 Mbps)) links to the Internet Service Provider (ISP) that are totally independent and provide for redundancy. The core backbone network is made up of Cisco routers and layer 3 Cisco Switches.

2.1 Network Roles and Responsibilities

- **GSA-IT Building Technology Services Division (BTSD) Technical Project Manager:** The BTSD Technical PM is responsible for all Information Technology Systems within the Public Buildings Service and facilitates, including the review and approval of network design diagrams with the Network Team. The regional BTSD Technical PM and the government sponsors/project POCs are the main point of contact, coordinating all activities between project managers and the Network Team.

- **GSA-IT Network Operations and Management Team (Network Team):** The Network Team manages the wide and local area networks (GSA WAN and GSA LAN). They are responsible for the entire IP transport layer to include all routing and switching equipment and access to IP connectivity. They have command responsibility for the GSA Wide Area Network (WAN) and GSA Local Area Network (LAN). They are also the sole provider for IP ranges and all IP addresses for devices associated with its network will be assigned by the BTSD Technical PM. The Network Team also responds to network access and issues relating to IP connectivity.

- **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.

2.2 GSA Network and Uptime

There are nuances associated with network "up time" in general. Rather than getting caught up in percentages and decimal points, it's important to know that GSA-IT strives to have the network up and available. During an unplanned outage, the network team takes the lead in managing and troubleshooting the outage with the various stakeholders. With that said, our approach should always be to have a Building Recovery (BR) plan in place to ensure continuity of operations. 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 in order to manage the system manually.

2.3 Standards for Interoperability

The following is a high-level list of items to consider for the implementation of an appropriate network design. ***Please Note: Hardware will not be deployed on the GSA network unless a network diagram is submitted by the project team and is reviewed and approved by the network team. Diagram reviews and feedback are coordinated through the BTSD Technical PM, for that region.***

- GSA-IT Network Team will support the entire IP transport layer from the point of network access, (i.e. GSA router) all the way to the point of demarcation, which is conceptually defined as the connection point to the vendor-provided gateway (IP addressable device(s)). This gateway on the aforementioned IP network is the gateway to the secondary protocol network, which supports the vendor-provided building system devices and components. ***Please Note: Secondary protocol could also be IP based. All secondary protocol networks must be LAN based and not connect to a commercial circuit. See 1.2.1 for details on how doing so will violate TIC policy.***

- Prior to release of a statement of work (SOW), issuance of a Request for Proposal (RFP) and/or a contract, a proposed network diagram needs to be submitted to the BTSD Technical PM to be reviewed with all concerned parties. Feedback on the network diagram will be provided within 10 business days of submission.

- BAS 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.

- Wireless technologies must have a minimum of AES 128 encrypted level, ideally 256 bit AES encryption is preferred.

- Government agencies are required to use FIPS-compliant encryption, regardless of the technology that is using them. While this requirement may not be available and/or affordable, GSA strives to select FIPS-compliant products and continues to advocate and motivate the building systems industry towards having solutions validated against FIPS 140-3.

- All switching and routing hardware will be provided, managed and maintained by GSA-IT Network Team.

- Vendor-provided intermediary devices such as media converters, hubs, switches and routers **will not** be allowed on the GSA network. Switches provided by GSA-IT Network Team are configured to detect and disengage with such devices on the network.

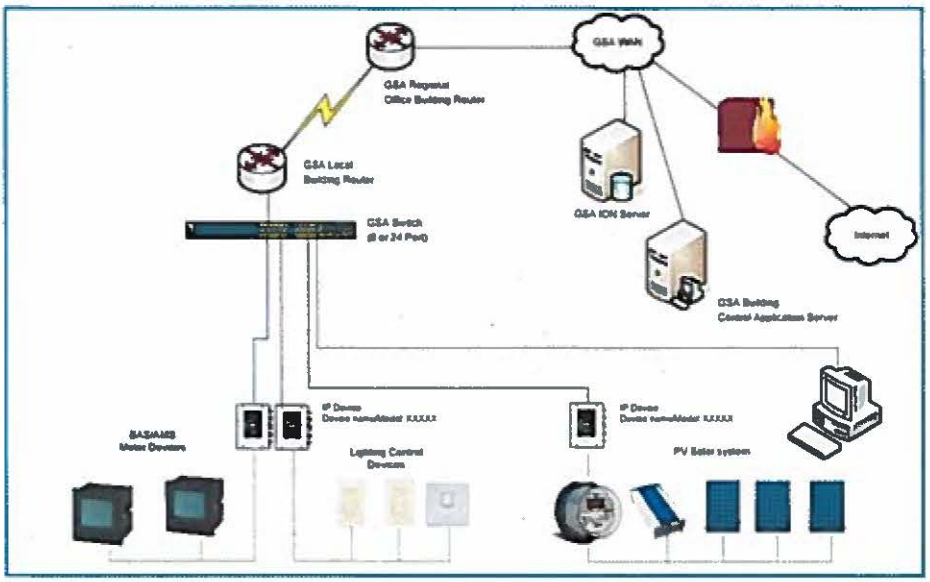
- Where possible, the same network gear is leveraged to support all approved agency hardware, including but not limited to user workstations and BMC devices.

- 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 Device and Application Security Assessment Process.***
    - All devices on the GSA network are subject to continuous monitoring and periodic scanning by GSA-IT.
    - All whitelisted devices must connect to a GSA switch. ***Please Note: See Section 1.2.3 for details on the BMC Device Whitelisting Process.***
- Additional switch(es) will be provided to accommodate new projects if the existing switch(es) is inadequate. (i.e., port saturation, distance).
- Switches should be connected using the assigned trunk port only.
- Only GSA-furnished hardware is permissible (i.e., workstation, server, routing and switching).
- All IP ranges/addresses will be provided by GSA-IT Network Team, in coordination with the PB-ITS BTSD Technical PM.
- Subnets cannot be provided before knowing the quantity of IPs, device models and a network riser diagram.
- For new installations, GSA-IT prefers the local vendor to complete the cabling for all IP enabled devices back to the GSA provided switches, in accordance with the GSA Telecommunications Distribution Design Guide (TDDG). Maintenance and repair of cabling is the responsibility of facilities management staff.
- In order to migrate an existing cabling infrastructure to a GSA-approved system, cabling may need to be restructured. In the cases where existing contracts with the vendors have expired, BTSD will provide technical guidance according to TDDG. Building Management is responsible for the cost of labor and materials.
- Network diagrams must be reviewed and approved by the GSA-IT Network Team before network hardware can be configured and sent to the site.
- For existing implementations (retrofit), the project team needs to ensure that any non-standard switches and router(s) are replaced by GSA Government Furnished Equipment (GFE) switches and routers provided by GSA-IT Network Team.
- All Ethernet (IP enabled) devices need to terminate at a GSA switch.
- All IP based traffic will be managed and maintained by GSA-IT Network Team.
- All IP based MAC addresses will be required to be entered/whitelisted in Cisco Identity Service Engine (ISE) database, prior to installation.
- Per the P100, Chapter 7 - Fire Alarm and Emergency Communication Systems: "With the exception of 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.
- All contractors who require access to GSA hardware, network and/or systems, must become a credentialed GSA user on the ENT domain. Preliminary adjudication of the National Agency Check with Written Inquiries (HSPD-12) clearance is a mandatory prerequisite for this access.

- No data will be transmitted outside the GSA network without government approval. Government sponsors/project POCs need to ensure vendor personnel maintain their ENT accounts and keep them active, in order 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.

2.4 Network Topology

The following figure is not intended as a network diagram, but rather a topology that demonstrates an example of logical interconnections amongst vendor-provided devices and the GSA LAN and WAN. This example provides a foundational approach for the design of an integrated building controls and/or energy system.



2.4.1 Network Design Requirements

Items that need to be addressed in the drawings sent to the GSA-IT Network Team shall include the following considerations:

- Switches will be deployed based on geographic layout of the building and disbursement of network nodes. Typically, it is not necessary to deploy a switch on every floor. Rather, hardware from adjacent floors can be connected to switches on adjacent floors, provided it is within the attenuation limitations maximum distance (IEEE standards (100m/328 ft).

- It is desirable that Access switches be connected via home run to the Core/Distribution switches. Daisy chaining switches is strongly discouraged. However, it may be approved by the Network Team on a case-by-case basis if both of the following conditions exists:

    - If it is cost prohibitive or not technically feasible to connect Access layer switches directly to Core/Distribution switches via home run.

    - If the daisy chained switches do not exceed a maximum of 3 hops from the Core/Distribution switch(es). ***Please Note: In cases where design or budget does not allow for home runs to the core switch, project owners 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.***

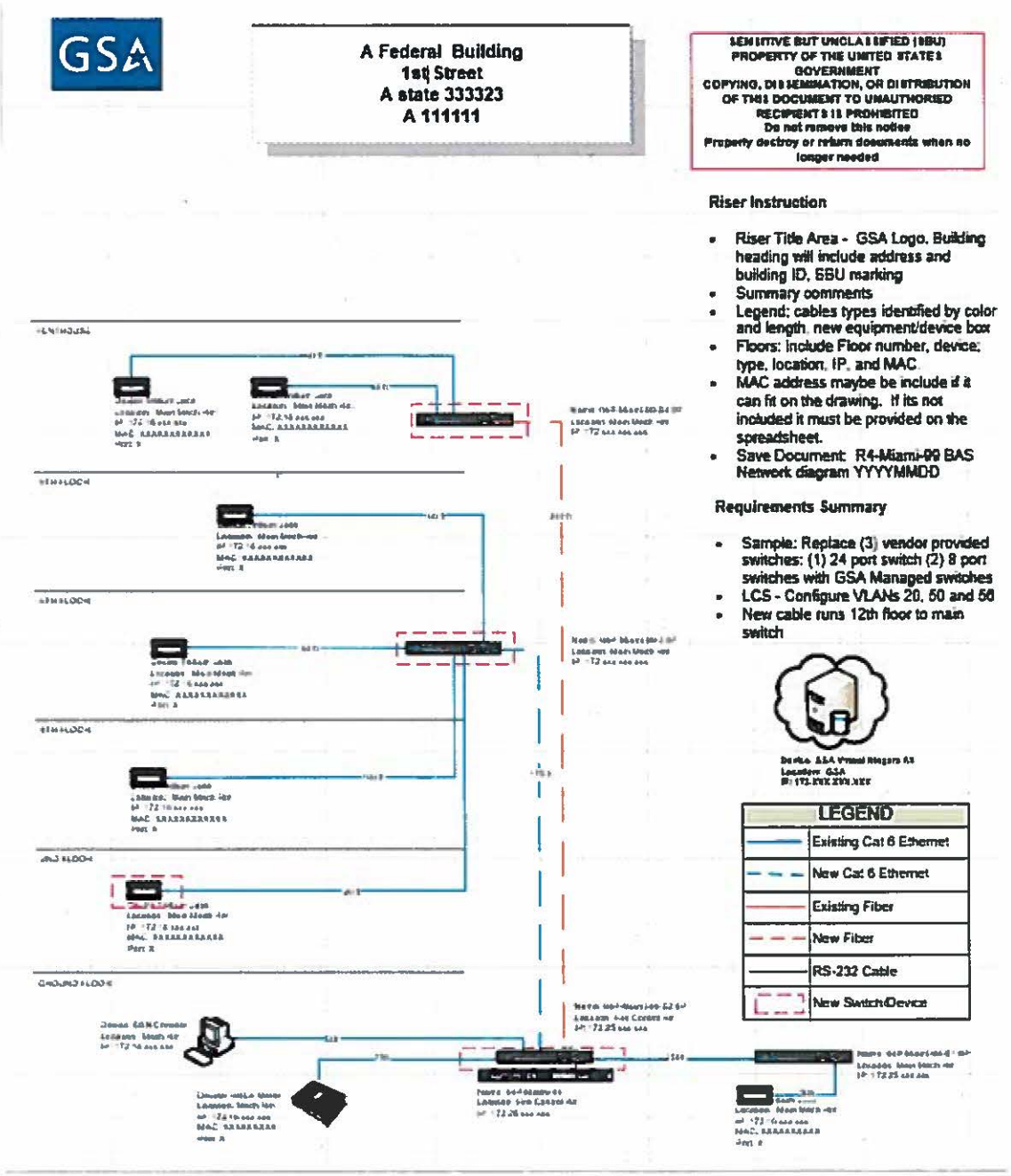
- As a rule of thumb, the drawings need to show devices, locations and cabling. In addition, it shall:
  - Clearly show every single IP enabled controller or component that the vendor is introducing
  - Include model information on the building automation controller or component that connects to the IP network
  - Show GSA switch and the path from each IP device to the switch location
  - Show cable runs, devices and GSA switches per floor
  - Network diagrams should reference the type of cable being used. Minimum standard for Ethernet is plenum-rated, Unshielded Twisted Pair (UTP), Cat5e (if adding to existing) cable. Cat6 certified RJ45 (M/F) and Patch Panels to be used Cat6 cable
  - Cable run lengths. Attenuation limitation is 100m/328 ft, which is safe for data transmission
  - If using a Fiber Optic riser to support intra-building network IP connectivity, detail the Type (Single or Multimode), Shielded/Armored and type of Endpoint. Be sure to display how that fiber is connected through the building, and specifically which strands of fiber are being used at each connection point
  - Fiber Optic runs are required for switch-to-switch connections between floors if distance exceeds 328 ft.
  - Port density requirements for GSA switches are to be accurately represented

Please Note: Sensitive but Unclassified (SBU) notice must be included on network diagrams.

SENSITIVE BUT UNCLASSIFIED (SBU) PROPERTY OF THE UNITED STATES COPYING, DISSEMINATION, OR DISTRIBUTION TO UNAUTHORIZED RECIPIENTS IS PROHIBITED Do not remove this notice Properly destroy or return documents when no longer needed

2.4.2 Sample Network Design Diagrams

The following is a sample depiction of an acceptable network design diagram. The diagram illustrates a floor-by-floor depiction, which includes wiring and location of hardware. 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.



2.5 Hardware Standards and Policy

All switching and routing equipment will be provided by the GSA-IT Network Team. Only approved Government Furnished Equipment (GFE) is allowed connection (i.e., Ethernet) to the network unless specifically approved, in writing, by the authorizing official. ***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 a GSA Circuit

Before any project begins, the government sponsors/project POCs must confirm if a GSA circuit exists at a site. If not, they must order a GSA circuit first since the installation process typically takes 120 days (barring no issues) from the day that the order is submitted by GSA-IT (not when the SN 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. In order to submit a request for a circuit, the government sponsor/project POC must:

- Login to [redacted] (need to be either on VPN or use 2-factor authentication).
- Type "circuit" in the search bar and select "New Circuit Request".
- Complete all required fields and submit a ticket. Please contact the BTSD Technical PM for any questions.
- The ticket will go to the requester's supervisor for approval. They will receive an email and can approve directly within the email.
- Provide the ticket number (which will start with REQ or RITM) to the regional BTSD Technical PM.
- After submitting the ticket, please contact [redacted] or the regional Customer Service Engagement Champion if there are any additional questions.

2.5.2 Requesting Switches and Routers

GSA-IT Network Team needs to be involved early in the process, prior to when the award is made, so that they can provide switches and routers in a timely manner. Although switches and routers are sent from Network Team, the requests need to be routed through GSA-IT and BTSD. Once the network diagram is approved and the site's data circuit availability is confirmed, the switch(es) and the router(s) will be sent to the site. GSA-IT and the BTSD Technical PM will discuss the switching and routing needs with the various project teams before the hardware is shipped.

2.5.3 Configuration and Connection of the Switches and the Routers

The project team is expected to work with regional GSA-IT Deskside Services to physically set up the switches and routers in their designated locations. To configure a port on the switch, contact the Network Team by submitting a ServiceNow ticket for a Change Order to be created. ***Please Note: Switch installation can be completed by the vendor, Deskside Services or SmartHands (GSA contract with a fee associated with PBS) with the coordination of The Network Team and BTSD.***

2.5.4 Acceptance of Non-Standard Hardware

All hardware designed for implementation must be scanned and approved by the GSA-IT Security prior to implementation. ***Please Note: See Section 1.4 for details on the BMC Device and Application Security Assessment Process.***

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 its primary use is in HVAC applications, the BACnet standard can support other building control systems such as life safety, security and lighting.

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" or 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:** 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 the 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:** Virtually everyone has heard the term TCP/IP. This is the term often generically applied to anything on the Internet or anything using "standard" networking. The UDP side of the stack operates in parallel to TCP and is automatically included in most implementations of an Ethernet based protocol stack. The difference is that 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. UDP 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. TCP is used when the data integrity and the order in 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:** Is a BACnet device that connects two or more networks, or two or more segments of a single network.

- **BACnet Broadcast Management Device (BBMD):** 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 SLIP or 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. And in this sense, 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 be sure to avoid when implementing BACnet on the GSA WAN. First, it is important that all device instances associated with a BACnet network are unique. 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 B/IP network, there may be occasions when it is desirable for two collections of B/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 B/IP networks has been coordinated. For example, it is assumed that device object identifiers are unique "internetwork wide." If this is not the case, the 'Who-Is' service will produce ambiguous results. Similarly, the 'Who-Has' service may be useless for dynamic configuration applications if multiple instances of objects with identical object identifiers exist. Second, issues can arise when BACnet objects that are not associated with each other share a broadcast domain. For example, 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, this is a scenario likely to occur. In this scenario 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.

Contractors are required to change from the default UDP port and ensure they are not using a UDP port assigned to any other region. 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 (but 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 B/IP network consisting of two or more subnets shall have one, and only one, BBMD. Each BBMD shall possess a table called a Broadcast Distribution Table (BDT) which shall be the 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 to and from their virtually hosted application servers to and from the BACnet objects at each field site. 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. In order 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) and 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 (B/IP-M)

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.

Chapter 3

Cabling and Data Circuit Installation/Upgrade

3.0 Overview

This chapter will provide guidance on cable installation to support the implementation of BMC Systems such as Building Automation Systems (BAS), Physical Access Control Systems (PACS), lighting control, Photovoltaic (PV) and Advanced Metering Systems (AMS). Additionally, it will establish the roles and responsibilities between vendors and GSA-IT, to ensure GSA's standards are met and questions on the agency's standards on cabling are answered. This chapter will primarily focus on guidance on Ethernet cabling, which includes Cat 5e, Cat 6/6a and Fiber Optic cabling for IP Based components. For questions regarding cabling for local BAS (BMC) networks, consult with the "Building Automation Systems" chapter of the Telecommunications Distribution Design Guide. Lastly, this chapter will detail the data circuit installation process. Ultimately, this guide is related to any installations that require IP network connectivity.

3.1 Applicable Standards for Cabling Infrastructure

All cabling in the GSA buildings needs to be done in accordance with the BICSI standards and is in conjunction with the GSA Telecommunications Distribution Design Guide (TDDG), as it relates to Ethernet cabling. All other types of cabling installations will be handled on a case-by-case basis.

3.1.1 Minimum Requirement for Ethernet Cabling

Cat 6 cabling is the minimum standard for new Ethernet cabling. Please consult the Telecommunication Distribution Design Guide (TDDG) for the latest cabling requirements as the cabling categories are rapidly changing. ***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.***

3.1.2 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 328 ft., beyond this length, the signal quality may become unstable and transmission errors will occur. For cable runs longer than this length, GSA-IT will likely recommend a fiber run.

3.1.3 How are GSA-IT's Cabling Standards Enforced?

Any cabling that will provide the medium of connection between a GSA furnished router or switch to a device that resides on the GSA LAN will be subject to a review and approval process, as specified in the TDDG, by GSA-IT. All other cabling components are to comply with Industry standards as specified in the TDDG. Any installation with GSA-provided IP address wiring back to the GSA switch, is to follow the TDDG and the approval process. Any issues with cabling installed by the vendor will need to be addressed by the vendor that has installed the cabling. 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.

3.2 Cabling Installation

This section will describe the roles and responsibilities involved with installing network cabling as well as GSA-IT's cabling requirements in a network design diagram. It will also discuss the several approaches for cabling, depending on stage and location of the BMC project.

3.2.1 Cabling Installation Roles and Responsibilities

- **Vendors and Contractors**: Provide and install all network cabling. ***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.***

- **GSA-IT**: Is responsible for all GSA IP traffic and will support all associated network cabling once it is installed and accepted. Will serve as the point of contact for the projects regarding proposed cabling design and questions about standards. Will work with the projects and vendors to effectively communicate standards, answer questions and provide guidance from the beginning of the design phase all the way through installation.

3.2.2 General Architecture

Please Note: See Section 2.4.1 for GSA-IT's cabling requirements in a network design diagram.

3.2.3 Cabling Installation Options

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:** In order 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.

3.2.4 Cable Installation Support

GSA-IT encourages project managers to let vendors handle all cabling for controlling devices, metering devices and building controllers, 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.***

3.3 Data Circuit Installation

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 minimize any unnecessary additional cabling or 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 and will extend the delivery time of the completed circuit and sometimes push the project timeline out considerably.

3.3.1 Data Circuit Installation Roles and Responsibilities

- **The Requirements Analysis Team:** Vets the data circuit installation requests; verifies all the provided information including the location of provided phone numbers and addresses are correct; the listed site POC is contacted and knows about the upcoming installation; collects quotes for installation and provides recommendations; and submits requests to the Telco vendor.

- **Site Point of Contact:** This person is present to let the vendor into the building on the scheduled site visit, confirm the correct site telecommunications address, and escort the Telco vendor.

- **Telco Vendor:** Provides quote for circuit installation and sends order to the RA team for review. Subsequently, they will install the circuit and help with troubleshooting and connectivity issues.

3.3.2 Process for Data Circuit Requests and Sites Visits

- Data circuit installation requests are submitted via an email from the BTSD Technical PM for the specific region to the Requirements Analysis (RA) team at [redacted] to begin the ordering process.

- The email needs to contain the mailing address for the building that the circuit will terminate in, a local on-site POC, telephone number that is located 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 RA team will call the POC listed to validate all information provided and to ensure the POC is aware of the requirement so there is no confusion when the Telecommunications Carrier or the Telephone Company (known as "Telco") contacts them for access to the facility.

- The RA team for GSA-IT places an order with the telecommunications service provider for a new or an upgraded circuit at a specific location.

- The provider has 60 days from order acceptance, provided they've been given all the information they require, to have the circuit operational and ready for use. There are several definable steps that either must or can happen to deliver this circuit.

- At every location there is a Local Exchange Carrier (LEC) that has ownership of the telecommunications infrastructure at that building. If the LEC is a separate company from the one that the original order was placed with, like Verizon, then the provider will need to issue an order to the LEC to extend access from their closest point of presence to the termination point within the GSA facility.

- The 1st telco visit that will be made by a technician from the LEC will be to extend physical access from their point of presence (PoP) to the appropriate termination point in the GSA facility. In some cases, the existing contractual agreements may not be in place between the service provider and the LEC, and an additional visit will need to be made by a wiring contractor to do the work necessary to extend the telecom infrastructure to the GSA facility, which would constitute a 2nd telco visit.

- Once the physical access has been completed, the service provider will need to install their Channel Service Unit/Data Service Unit (CSU/DSU) device at the point of termination to establish service. This will require a separate visit, which could be the 2nd or 3rd, depending on how many visits were required to complete the physical access.

    - Telecommunications technicians' visits should be preceded by an agreed upon notification time not less than 24 hours to the GSA point of contact that was provided to them. It is usually the facility manager who serves as the point of contact, and that person may or may not be on-site already. In either case, an on-site federal employee or contractor in possession of their PIV-II Card must escort these technicians through the building and to the requested access points to complete their work. Failure to meet with the Telco technician may result in the rescheduling of the visit and

substantial delays of the process.

- Once service has been established, if the circuit requested was a new one, a GSA router will need to be installed at the site and connected to the (CSU/DSU). In some cases, a GSA staff member will arrive on site to install the equipment, they will require access to the CSU/DSU, to complete the installation. In many cases, the router will be shipped to the building, and someone on-site will be asked to plug in the router and connect it to the CSU/DSU. There is support available in Central Office to walk on-site staff through the installation of the GSA router. Support for installation will be coordinated through the PB-ITS' ACT Team.

3.3.3 Important Considerations in the Circuit Installation Process

Circuit installation shall follow the guidance of the TDDG. The local POC and the installing contractor shall be aware of this requirement.

- It is crucial to identify a local point of contact that is available to meet with the vendor when they arrive on the scheduled day of visit.
- A good address for the site location is critical in this process. A physical address is not always the same as the telecommunications address. A "good address" would be an address verified from the postal service website, Google Maps or Bing Maps. Also listing any historical addresses for a location is also important. Any issues with address may affect the installation timeline.
- Circuit installation shall follow the guidance of the TDDG.

Chapter 4

BMC Servers: Standards, Provisioning, Application Installation, Maintenance and Remote Access

4.0 Overview

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

4.1 BMC Server Roles and Responsibilities

The Technical Operations Team (TechOps) provides guidance to the PBS organization for IT hardware, OS, database and security compliance within the GSA standards for BMC, national, and regional applications for PBS systems. Below is the contact information about the TechOps Team.

- **Email:** [redacted]
- **Phone:** 866-274-0781
- **Hours of Operation:** 7am - 7pm Eastern Standard Time
- **Website:** [redacted]

Please Note: Forms and other information can be found on the PBS Portal website under the "BMC" tab. This site is only available within the GSA firewall.

4.2 BMC Server Standards

The GSA provides virtual servers to host building monitoring and control applications. To help meet the energy efficiency goals of the GSA and move towards a virtual environment, it is standard practice for TechOps to provide VMWare virtual servers 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 applications:

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

- Executive Order (EO) 3514, signed in October 2009 by President Obama to "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 is the touchstone for the GSA's work in sustainability, giving the GSA the responsibility and opportunity to find solutions, in partnership with other agencies, to drive energy and cost savings throughout government. This EO also began GSA's journey to the former Administrator Martha Johnsons' Zero Environmental Footprint (ZEF).

- The GSA's 2010 Sustainability Plan 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. As part of the BMC application server virtualization effort, GSA-IT leadership met with various vendors to ensure virtualization is possible with their solutions deployed at GSA.

Please Note: GSA-IT no longer provisions 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; this 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 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.

The BMC server hardware specifications are:

- Hypervisor vendor: VMware
- Memory: 8 GB

- CPU: 2 vCPUs
- Hard Drives
  - System Drive: 100 GB
  - Application Data Drive: 100 GB

The BMC 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 Technical PM for the latest BMC server build specifications.

4.2.3 BMC Application Requirements

Requirements in order 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 software credentials

GSA-IT will not accept BMC 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 Technical 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.

4.2.4 Server Security Hardening

Security measures are implemented on all servers and applications to prevent security breaches which can result in loss of server availability or data. To that end, TechOps will harden the operating systems, web server and database with CIS Benchmarks [redacted].

After the contractor/vendor installs the BMC application, TechOps will perform an application and database scan. BMC applications must be hardened and follow the Security Assessment Report (SAR) which can be provided to the vendor/installer by the regional BTSD Technical PM or PBS project POC(s). TechOps performs regular scans of BMC production servers and reports on discovered vulnerabilities. It is the

responsibility of the PBS project team to ensure the vendor has applied the necessary hardening, as prescribed in the SAR. ***Please Note: it is strongly encouraged to include Software Maintenance Agreements (SMA) for applications so that security updates and patches can be applied in a timely manner during the lifecycle of the application. Failure to resolve critical and high findings in a timely manner may result in decommissioning of the server/or removal from the network and will be the responsibility of the PBS project stakeholders.***

4.3 BMC Deployment Process

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

4.3.1 Step 1: Submit BMC Server Request Form

Prior to submitting a BMC Server request, please ensure that all BMC software has been remediated by IT Security. Once the SAR is disbursed, complete a BMC Server Request Form found on [redacted] Please coordinate completing this form with the vendor and submit it to the regional BTSD Technical PM. Provide the following supporting documentation (if available):

- Application installation instructions
- System configuration guide
- Technical specification guide
- Architecture design diagram (Visio diagram preferred)

4.3.2 Step 2: Schedule Server Solutions Meeting with TechOps

- Schedule a meeting with TechOps by using the [redacted] or contact TechOps by email at [redacted] to request a Server Solutions Meeting. The instructions for how to schedule an appointment are [redacted]
- The person(s) that will install the BMC application must be present in the Server Solutions Meeting. The stakeholders that should attend the Server Solutions Meeting are:
    - Regional GSA POC(s) (mandatory)
    - Regional Technical POC (if any, optional)
    - Facility Manager (optional)
    - Vendor assigned to install the application (mandatory)
    - Vendor assigned project managers (optional)
    - TechOps team member (mandatory)
    - BTSD Technical PM (optional)
    - Regional Building IT Specialist (RBITS) (optional)

TechOps will review the form and plan out the architecture with the project's stakeholders. Once all parties have agreed that a server is needed, TechOps will provide an estimated server delivery date.

4.3.3 Step 3: Server Deployment Process

The server is built, configured, and hardened by TechOps. After TechOps completes these tasks, the server is made available to the Regional GSA POC for the vendor to install the application. All server builds include the following:

- Operating system installation and security hardening
- Database installation and security hardening
- Security and compliance measures
- Server component configuration

Standard server builds are typically completed within two weeks. Non-standard server builds may take longer.

4.4 Application Installation and Maintenance Guidelines

This section describes the roles and responsibilities, application installation guidelines and installation support options for the vendor to use when installing the application based on the SAR.

4.4.1 Installation and Maintenance Roles and Responsibilities

TechOps Team	Regional Building/Project POC

• Architecture design
• Server deployment
• Windows component installations
• Patching for OS and DB
• Resolve OS and DB vulnerabilities
• Install and configure OS and DB
• Provide server access
• Assist installer with copying over BAS software installation files to the server
• Restart server
• Monitor application
• Overall security of solution
	• Application specific
	  ○ Install the application based on SAR
	  ○ Upgrades
	  ○ Patching
	  ○ Resolve application vulnerabilities
	• Application technologies
	  ○ Other web server
	  ○ Any other non-OS or DB component
	  ○ Devices

4.4.2 Do's and Don'ts for Application Installations

Do:

- Request HSPD-12 clearance; obtain Active Directory ENT account, and GSA email account from the regional government sponsors/POCs. This is a requirement to access any GSA server.
- Expect to only have temporary administrator access to the server during installation/maintenance periods.
- Use the E:\ (DATA) drive to install all software on virtual servers. Physical servers will only have C:\ drive.
- Contact TechOps for reboots.
- Request TechOps to install Windows Server Components.
- Provide any documents about the software being installed on the server to TechOps.
- Submit a [redacted] after installation is complete.
- Expect to participate in the server solutions meeting with TechOps. The meeting is required before a server is built.
- Send the software to TechOps to copy it on the server. This will avoid latency during the installation process.
- Expect the server to be patched and rebooted on a monthly basis at a minimum.

Do not:

- Upgrade BAS software patches/minor updates without GSA IT Security approval.
- Remove the server from the ENT domain.
- Use manufacturer default passwords.
- Create a local account on the server without consulting with TechOps.
- Reinstall the operating system.
- Rename the server.
- Change the IP of the server.
- 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.

4.4.3 Temporary Server Administrator Access Requests and Reboots

- Go to [redacted]
- Click on Self - Service Catalog.
- Type in "BSN" in the search box and select "PBS BSN Temporary Admin Remote Access".

- For instructions on how to fill out the ticket, please refer to [redacted]

4.4.4 Approval Authority Table

The table below identifies requests that require a GSA Government POC approval.

Request From	Server Temp Admin Access	Any RDP Access and Citrix VDI for Self or Others	Server Reboot
GSA-IT Team	• Server Gov POC(s) must approve • Request from ServiceNow	• No approval needed • Request from gsa.gov email only • TechOps will copy relevant stakeholders	• No approval needed • Request from gsa.gov email only • TechOps will copy relevant stakeholders
Any POC	• Server Gov POC(s) must approve • Request from ServiceNow	• No approval needed • Request from gsa.gov email only • TechOps will copy relevant stakeholders	• No approval needed • Request from gsa.gov email only • TechOps will copy relevant stakeholders
Government POCs	• Self-approval permitted • Request from ServiceNow	• No approval needed • Request from gsa.gov email only • TechOps will copy relevant stakeholders	• No approval needed • Request from gsa.gov email only • TechOps will copy relevant stakeholders

4.4.5 Dedicated Server Support During Installation

If full attention from a TechOps server technician will be needed during the application installation, contact [redacted] and provide a date and time frame for the requested support.

4.4.6 Copying Files to a Server on the BSN

The requirements for copying files to a server on the BSN are:

- GSA ENT account
- Citrix VDI access
- Server RDP access
- SecureAuth (instructions are on [redacted]
- Permissions to access the [redacted] shared network drive (granted by TechOps)

Different methods of copying files to the BSN:

- Copy files from a GSA workstation to the [redacted] shared network drive. Then, copy files from the shared network drive to the server desktop.
- Email files to [redacted] if less than 25 MB.

- Provide a download link for TechOps to download the media.
- Mail the media to TechOps (contact TechOps for a mailing address).
- Use the TechOps SFTP server to transfer files outside the GSA Firewall to external servers. SFTP requirements must first be discussed with TechOps.

4.4.7 Simple Mail Transfer Protocol (SMTP) Email Server Information

- SMTP refers to the ability for applications and devices to send email notifications through the GSA email server to any email address internal or external.
- In the application or device configuration, enter the following details:
  - SMTP Server:
    - [redacted] (for use with applications and servers)
    - [redacted] (for use with devices or building consoles)
  - [redacted]
- Authentication: No authentication is needed
- From address: any email address with gsa.gov suffix (For example: [redacted])
- To address: any valid email address specified

4.5 Application Access

There are two ways to access an application using either a BSN console or Citrix VDI: via web browser or Remote Desktop Protocol (RDP). The preferred method of access is via web browser (i.e., Niagara Web Access). For applications that cannot be accessed directly via web browser (i.e., Niagara Workbench, Alerton Compass, Siemens Desigo, etc.), RDP shortcut links can be used in Citrix VDI to directly login to the server. This section will describe how to request server access and how to access an application.

4.5.1 Methods for Accessing an Application via Web Browser

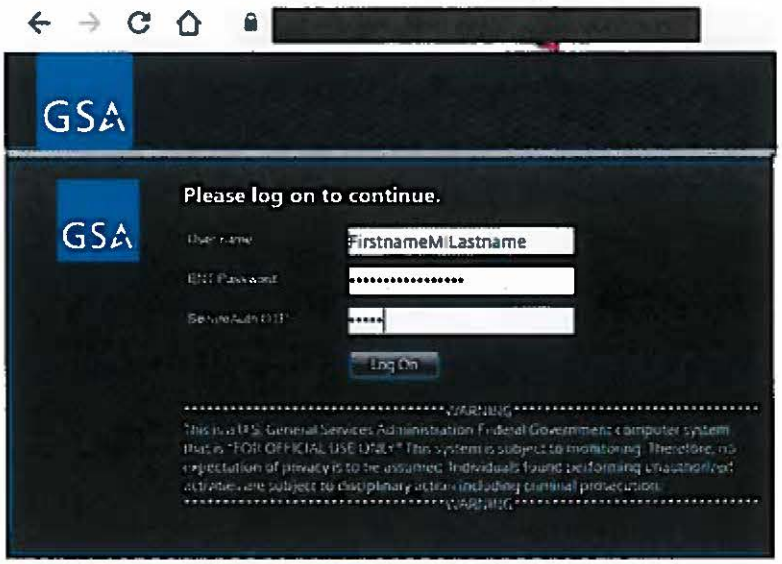
Web browsers are the preferred method for accessing any BSN application.

4.5.1.1 How to Request Access to a Web Application

Contractors requiring access to BMC system servers must work with their government sponsors/project POCs in order to obtain proper clearance and the necessary credentials before system access can be granted by GSA-IT.

4.5.1.2 How to Access a Web Application via Citrix VDI

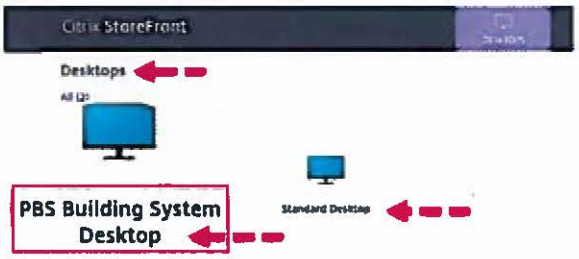
- Open a web browser and go to [redacted]
- Enter ENT username, ENT password and OTP code.



If this is the first time connecting in from a web browser, there may be a prompt with a "Welcome to Citrix" window.

- There are two options to select from:
  - **Detect Receiver:** Clicking the "Detect Receiver" button will attempt to detect if the Citrix client is already installed. If it finds the client, the available Citrix VDI desktops will show up.
  - **Light Version:** Clicking "Use light version" opens the HTML5 (web) version of Citrix VDI. Use this version if the Citrix client is not installed or administrator privileges are not available to install it.

- The Citrix VDI Desktops available will be presented.



- Click and open the "PBS Building System Desktop" to launch the VDI desktop.

- Open the web browser (either Chrome or IE) and type in the URL of the BSN application. Credentials to the application should have been provided by the regional government sponsor/project POC.

4.5.1.3 How to Access a Web Application via BSN Console

- Login to the BSN Console. ***Please Note: See Section 1.5.6 for details BSN Console credentials.***
- Open a web browser (whether it's Chrome or IE).
- Type in the URL for the application.
- Log into the BSN application with the credentials supplied by the government sponsor/project POC.

4.5.2 Methods for Accessing an Application via RDP to a Server

RDP access should be limited to applications that cannot be easily accessed via web browser.

4.5.2.1 How to Request RDP Access to a Server

- Contact [redacted] using a gsa.gov email.
  - Specify server name or IP address.
  - Specify the user's ENT account (i.e. ENT\JonASmith) that needs to have access.
  - Provide an "end date" if the remote desktop access should be removed by a certain date.

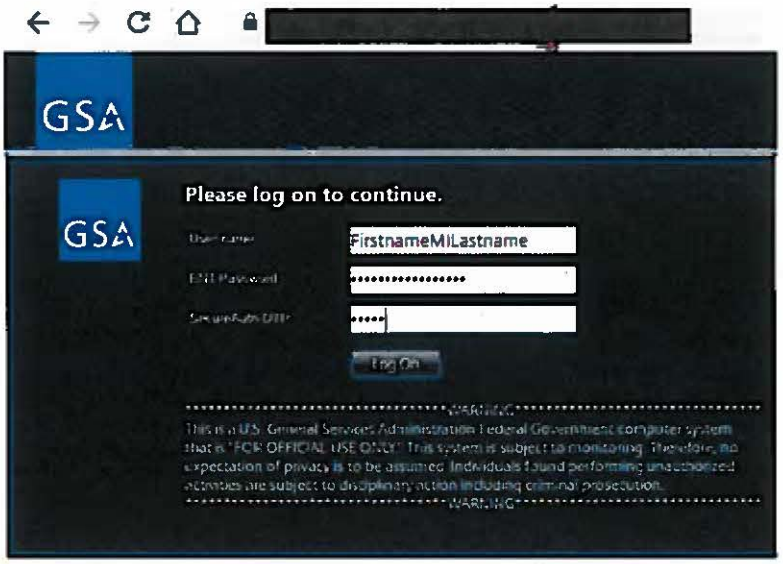
TechOps Windows Server Access Requirements:

	Remote Desktop User ("RDP")*	Temporary Windows Administrator
Approval required by system owner (GSA Employee)	Yes	Yes
HSPD-12 clearance required	Yes	Yes
ENT account and GSA email required	Yes	Yes
Duration	Unlimited	Limited to 10 business calendar days at a time (weekends and Holidays excluded)

Please Note: Permanent Windows Server Administrator access is not permitted. See Section 4.4.4 for server access Authority Approval Table.

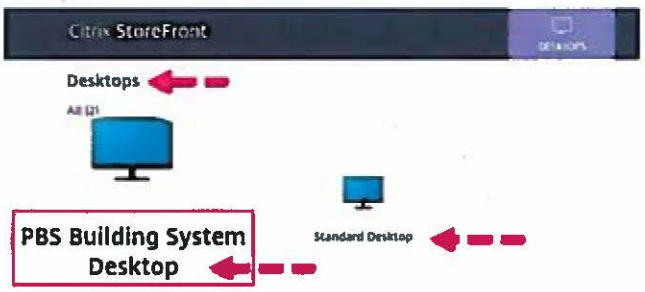
4.5.2.2 How to RDP to a Server via Citrix VDI

- Open a web browser and go to [redacted]
- Enter ENT username, ENT password and OTP code.



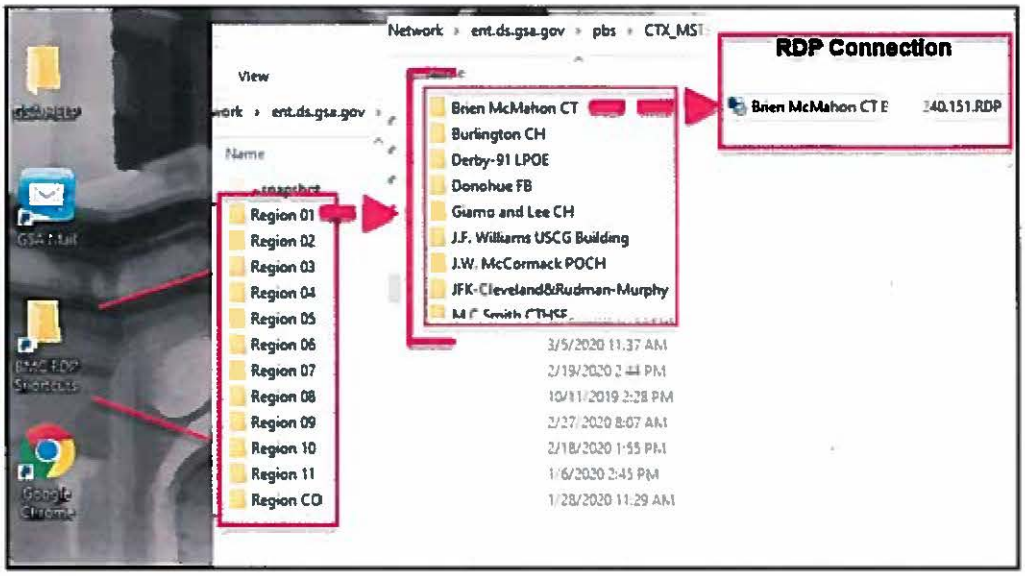
- If this is the first time connecting in from a web browser, there may be a prompt with a "Welcome to Citrix" window. There are two options to select from:
    - **Detect Receiver:** Clicking the "Detect Receiver" button will attempt to detect if the Citrix client is already installed. If it finds the client, the available Citrix VDI desktops will show up.
    - **Light Version:** Clicking "Use light version" opens the HTML5 (web) version of Citrix VDI. Use this version if the Citrix client is not installed or administrator privileges are not available to install it.

- The Citrix VDI Desktops available will be presented.

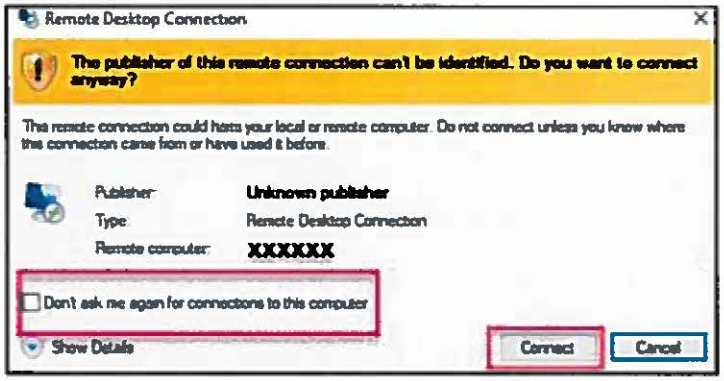


- Click and open the "PBS Building System Desktop" to launch the VDI desktop.

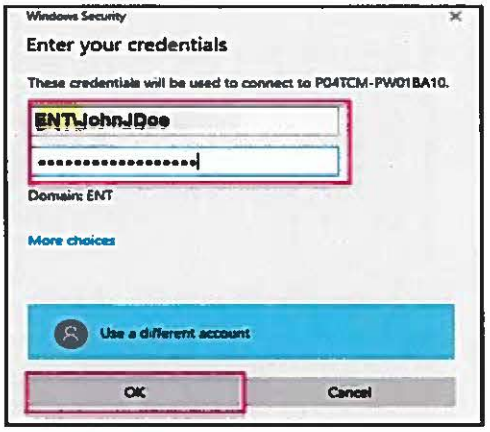
- Open the BMC RDP Shortcuts folder on the VDI desktop.
- Open the correct regional folder.
- Open the correct field site folder.
- Click on the appropriate RDP shortcut link.



- For convenience, check the "Don't ask me again for connections to this computer" box. Then click "Connect" to continue.



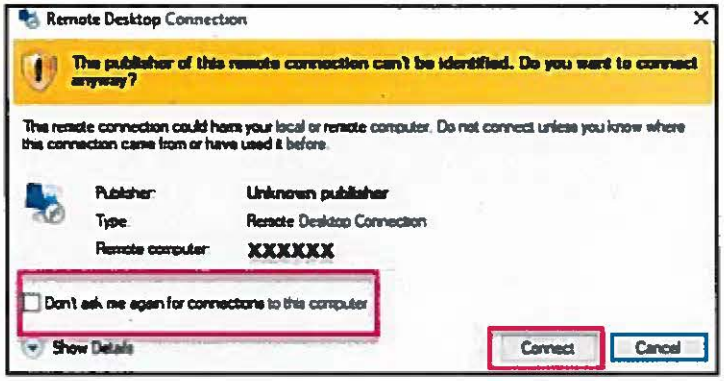
- On the next screen, enter ENT credentials to connect to the BAS server. Click "OK".



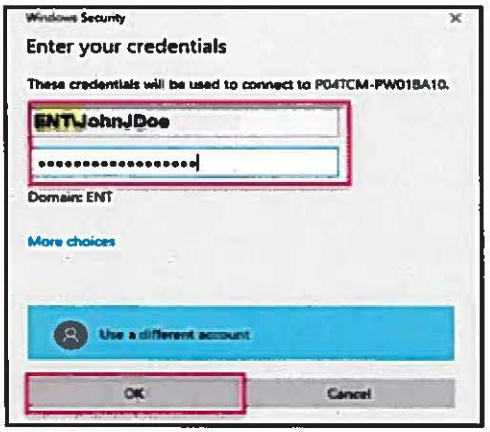
- Once on the server desktop, login to the application using the supplied credentials.

4.5.2.3 How to RDP to a Server via BSN Consoles

- Login to the BSN console using the supplied credentials.
- Open the server RDP shortcut on the BSN console.
- For convenience, check the "Don't ask me again for connections to this computer" box. Then click "Connect" to continue.



- On the next screen, enter ENT credentials to connect to the BAS server. Click "OK".



- Once on the server desktop, login to the application using the supplied credentials.

4.5.2.4 How to Log Off a Remote Desktop Session on a BMC Server

- Right click the "Start" button from the bottom left corner.
- Hover over "Shut down or sign out".
- Left click "Sign Out".

Please Note: Disconnect should be avoided as it stops the desktop but leaves the session open which consumes resources on the VDI host.

Chapter 5

Technical Support for BMC Systems

5.0 Overview

The GSA-IT service desk vendor is not structured to support BMC related calls/issues. As such, PB-ITS' TechOps triages any BMC support related issues. Facility managers, project managers, energy coordinators and all other stakeholders involved in BMC projects, will work with the PB-ITS TechOps to address technical issues. This chapter outlines BMC systems maintenance and support.

5.1 Technical Support Roles and Responsibilities

- **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 servers and patching the servers and consoles.

- **GSA-IT Network Operations and Management Team (Network Team):** The Network Team is responsible for troubleshooting the entire IP transport layer including all routing and switching equipment and access to IP connectivity. They are also responsible for managing network devices (switches and routers) on the GSA network, the BSN and the BSN Access Control List (ACL).

- **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 activities such as surveying cable connections, restarting/rebooting hardware, and the installation of hardware (network switches, BSN consoles etc.) as instructed by GSA-IT.

- **Controls Vendor:** If GSA-IT has determined that the issue resides with building control system 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.

- **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.

5.2 Server Maintenance and Support

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

5.2.1 Server Monitoring

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 [redacted] is submitted for the server,

except for 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
- Average Response Time
- Page Size

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

5.2.2 Server Backup Solutions

The backup solutions for virtual and physical servers are described below:

- **Virtual Servers:** 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 Monday through Friday and retained for 30 days. Weekly backups are retained for no more than 60 days.

- **Physical Servers:** NetApp has an agent called Open Systems SnapVault (OSSV), which is loaded on the production system to provide backup capabilities. The OSSV agent is configured to backup specific folder directories which it then snapshots back to one of GSA's data centers. Entire servers are not backed up. Folder and directory backups are performed Monday through Friday and retained for one year. ***Please Note: To set up a physical server backup, system owners must provide documentation that identifies key folders and directories.***

5.2.3 Server Patching

Most known vulnerabilities can be solved, and potential system attacks can be prevented by patching computers on a regular basis. TechOps performs Windows operating system patching on a monthly basis on the weekends. Microsoft's patch release day occurs on the second Tuesday of each month and is referred to as "Patch Tuesday". TechOps' development and test server patching occur four days after Microsoft's "Patch Tuesday". Production server patching is done two weeks after development server patching or 18 days after Microsoft's patch release day, "2nd Tuesday".

- Database patches are performed on a quarterly basis.
- Zero-Day patches are applied as soon as possible.

Please Note: It is recommended that the building POCs test their application for any issues on the Monday after BSN server patching. If any issues arise, report them to TechOps immediately.

5.2.3.1 Planned Maintenance and Outages

Any building POC (vendors, facility manager, project managers, etc.) should notify the TechOps of planned building outages or application maintenance in advance to avoid unnecessary troubleshooting.

TechOps will notify POCs/vendors on the regional lists below of any planned outage and include server names in the notification (if applicable). Access will only be granted to Government POCs. Please contact the regional BTSD Technical PM to request access. These lists also include information of the server, application installed, building affected, etc.

Region 1

[redacted]

Region 2

[redacted]

Region 3

[redacted]

Region 4

[redacted]

Region 5

[redacted]

Region 6

[redacted]

Region 7

[redacted]

Region 8

[redacted]

[redacted]

Region 9

[redacted]

Region 10

[redacted]

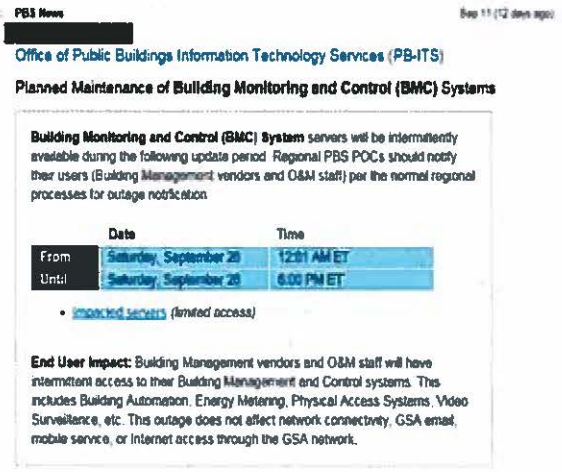
Region 11

[redacted]

Region 12/CO

[redacted]

Please Note: This is an example of what a planned maintenance notification email looks like.



PBS News [redacted]

Office of Public Buildings Information Technology Services (PB-ITS)

Planned Maintenance of Building Monitoring and Control (BMC) Systems

Building Monitoring and Control (BMC) System servers will be intermittently available during the following update period. Regional PBS POCs should notify their users (Building Management vendors and O&M staff) per the normal regional processes for outage notification.

	Date	Time
From	Saturday, September 26	12:01 AM ET
Until	Saturday, September 26	6:00 PM ET

- impacted servers *(limited access)*

End User Impact: Building Management vendors and O&M staff will have intermittent access to their Building Management and Control systems. This includes Building Automation, Energy Metering, Physical Access Systems, Video Surveillance, etc. This outage does not affect network connectivity, GSA email, mobile service, or Internet access through the GSA network.

5.2.3.2 Unplanned Maintenance and Outages

- **During business hours (Monday - Friday, 7am - 7pm Eastern Standard Time)**
  - If a Server Availability outage alert is received, TechOps will immediately start to troubleshoot the issue.
  - If TechOps can restore a server or service by restarting them, they will send an email to the Government POCs stating what was down and how it was resolved. They will ask the Government POCs to check the BMC application's functionality.
  - If restoration of the server or service cannot be resolved and TechOps has exhausted all efforts, the following actions will be taken:
    - For all servers, an email will be sent to the Government POCs stating what the issue is and what steps have been taken to that point.
    - For physical servers, TechOps will report the issue to the IT Service Desk and ask the on-site POCs to assist with troubleshooting.

- TechOps may have to involve other GSA-IT teams to resolve the issue (network team, Server Services, vendor, etc.)
- A request may be made by TechOps to have the software vendor help resolve the issue. It is the discretion of the Government POCs if that will be allowed.

- **After business hours (any time outside of days/hours listed above)**
  - TechOps will work to restore the server or service within one hour of when an alert is received. If the server or service is restored, they will send an email to the Government POCs and [redacted] stating what was down and how it was resolved. No phone call is necessary.
  - If restoration of the server or service cannot be achieved by TechOps after they have exhausted all efforts:
    - TechOps will call the listed Government POCs in order and will notify the first available person of what the issue is and what steps have been taken.
    - For physical servers, TechOps will report the issue to the IT Service Desk and ask the on-site POCs to assist with troubleshooting.
    - An email will be sent to the remaining Government POCs stating what the issue is and what steps have been taken to that point.
    - TechOps may have to involve other GSA-IT teams to resolve the issue (network team, Server Services, vendor, etc.).
    - A request may be made by TechOps to have the software vendor help resolve the issue. It is the discretion of the Government POC if that will be allowed.

5.2.4 Communications for BMC Contacts

When communicating to a mass BMC audience, TechOps will use [redacted] email groups for each region, and is maintained by the BTSD. Please contact the regional BTSD Technical PM to ensure all names are added to the distribution list to receive BMC related messages. Below are the email distributions groups by region:

- [redacted]

5.3 BSN Console Maintenance and Support

This section will describe BSN console patching and troubleshooting.

5.3.1 BSN Console Patching

TechOps performs Windows operating system patching on a monthly basis over the weekends. Microsoft's patch release day occurs on the second Tuesday of each month and is referred to as "Patch Tuesday".

- TechOps BSN console patching occurs four days after Microsoft's "Patch Tuesday" over the weekend.
- Zero-Day patches are applied as soon as possible.

Please Note: It is recommended that the building POCs test their application for any issues on the Monday after BSN console patching. If any issues arise, report them to TechOps immediately.

5.3.2 BSN Console IT Support

The TechOps triages BMC tickets for GSA-IT in ServiceNow. The general steps for BSN console IT support are as follow:

- A user contacts the GSA-IT Service Help Desk for help with a BMC related issue.
- The GSA-IT Service Desk will open a ticket for the user and route the ticket to the TechOps ("PBS Tops Energy" queue).
- TechOps will investigate the issue to determine whether it is a server issue, network issue, or console issue.
- If it is determined to be a console related issue, TechOps will transfer the ticket to the Regional Building IT Specialist (RBITS) team's queue, "PBS Buildings and Energy Systems Support".
    - TechOps may recommend the following actions for RBITS to take:
        - Provide end users with BSN Console logon credentials, logon instructions, and/or BSN console permission issues
        - Assist the IP address configuration on the BSN console or device, cable connectivity, switch configuration and other connection related issues
        - Coordinate downtime scheduling for BSN consoles directly with on-site staff
        - Console replacement for issues that cannot be resolved (i.e., hardware or operating system issues)
            - RBITS team works with the BTSD Technical PM to have BSN consoles replaced and sent to end users. ***Please Note: See Section 1.5.6.1 for more details on how to obtain a BSN console.***
        - RBITS will follow through with the issue and close out the ticket sent to their queue when the issue is resolved.
- TechOps will work tickets that are server related and close the ticket when the issue is resolved.
- Tickets that are network related will either be routed to the network team or TechOps will coordinate solutions with RBITS, server POCs, and any other teams necessary via email before closing the ticket.

5.4 BMC Issues

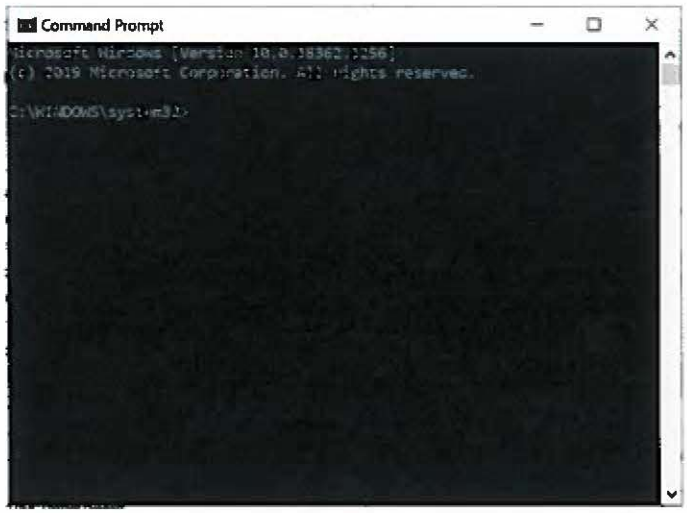
There are many reasons why a BMC system can be experiencing issues. This section will walk through basic initial troubleshooting steps, different methods to report BMC issues, how to describe a BMC issue and the BMC Systems Support Workflow.

5.4.1 Initial Troubleshooting Steps

This is meant to be a basic troubleshooting guide for connectivity issues. If this guide does not help solve the issue, a ServiceNow ticket may need to be submitted in order for it to be escalated to other groups.

Scenario 1: For any BMC hardware that is IP based and the device appears down or unresponsive

1) Inspect the device:
   a) Check if it is powered on/plugged in (must be powered on at all times).
   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.

(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 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)

5.4.2 Different Methods of Reporting a BMC Issue

There are four different methods for creating a ServiceNow ticket regarding BMC issues: call TechOps, email TechOps, call GSA-IT Service Desk Hotline or submit a GSA-IT Service Desk ticket with ServiceNow. This section will also go over how to describe a BMC issue.

5.4.2.1 Option 1: Call TechOps

- Call TechOps at 866-274-0781.

- Their normal business hours are 7am - 7pm Eastern Standard Time.
- After normal business hours, please leave a voice message with a name, call back number and a detailed description of the support issue. For emergency requests, TechOps will typically respond within an hour. 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.

5.4.2.2 Option 2: Email TechOps

- Email TechOps at [redacted] and copy the regional BTSD Technical PM.
- Their normal business hours are Monday - Friday, 7am - 7pm Eastern Standard Time.
- After normal business hours, TechOps will typically respond within an hour to emergency requests. 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.

5.4.2.3 Option 3: Call the GSA-IT Service Desk Hotline

Normal Business Hours:

- 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".

After Hours:

- Call 866-450-5250. An email to the ITSD after hours will not be seen until the next business day and in the order in which it was received.
- Select option 2 to report a critical enterprise-wide outage or service disruption. This option will escalate you to a person. The technician on the escalations line will have access to "on call" SMEs as needed and will get in touch with the appropriate escalation engineer(s).
- 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.

5.4.2.4 Option 4: Submit a GSA-IT Service Desk Ticket with ServiceNow

- Go to ServiceNow.
- On the left pane, click on "Service Catalog".
- Click on the option "GSA Generic Request - Didn't find what you were looking for?".
- Please fill in the "Short Description" field with a brief explanation of the issue.
- Please fill in the "Justification for Request" field with why help is needed from TechOps.

- In the "Additional Comments" field, input the following phrase: *Please route this ticket to the PBS TOPS Energy queue*. Then, use the next section as a guide to describe the BMC issue in the same field.

5.4.2.5 Describing a BMC Issue

When speaking with the support agent or composing an email, be sure to first mention that the issue is related to "Building Monitoring and Control Systems." Describe the issue, specify the type of system (i.e., building automation, lighting controls, etc.) and provide the following pieces of information:

- Server name and/or IP address
- Console name and/or IP address
- MAC address
- 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
- Application name and/or URL
- Building name
- Building number
- Address, city, state
- Network connectivity
- Desktop/software install
- Requesting hardware/IPs for a site
- Circuit installation or upgrade
- Application or device accessibility from workstation, BSN Console or Citrix VDI
- If possible, provide a screenshot of the error or what the error message says

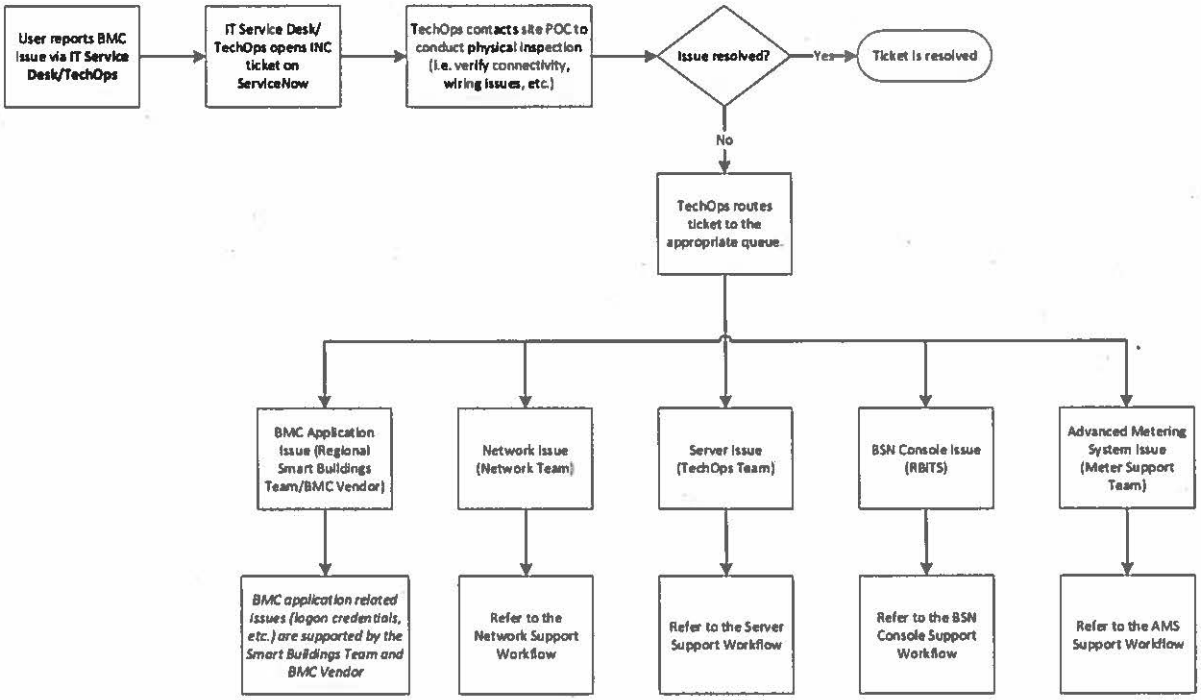
Examples of BMC, BAS applications/implementations to include on the call or email:

- Niagara (Tridium BAS application)
- Metasys (Johnson Controls BAS application)
- Desigo CC (Siemens BAS application)
- Quantum (Lutron lighting application)

5.4.3 BMC System Support Workflow

Below is an example of a typical troubleshooting workflow. Either the TechOps Team or IT Service Desk opens an incident ticket, which then the TechOps Team routes to other queues depending on the suspected issue. First, the TechOps Team will contact the site POC to determine if it is a physical issue. They will ask

the site POC to conduct a physical inspection by asking them to verify connectivity, check wiring issues, etc. If the physical inspection does not resolve the issue, then the TechOps Team will route the ticket to the appropriate team. The five main categories that issues typically fall under are BMC applications, network, server, BSN console, or an advanced metering system (AMS) issue.

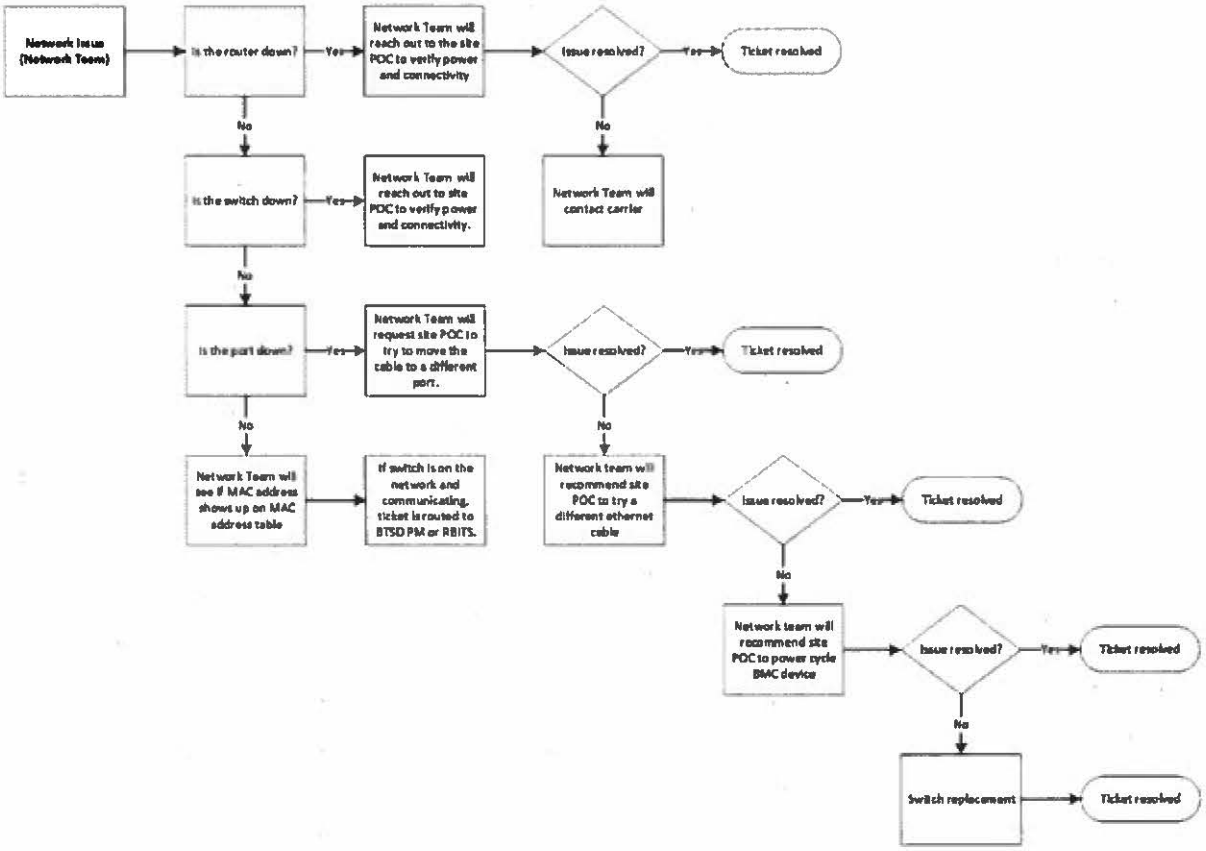


5.4.3.1 BMC Application Issue

Whenever the TechOps Team suspects that the issue is related to the BMC application, they will typically reach out to the Smart Buildings Team and the BMC vendor in order to troubleshoot issues such as login credentials, etc.

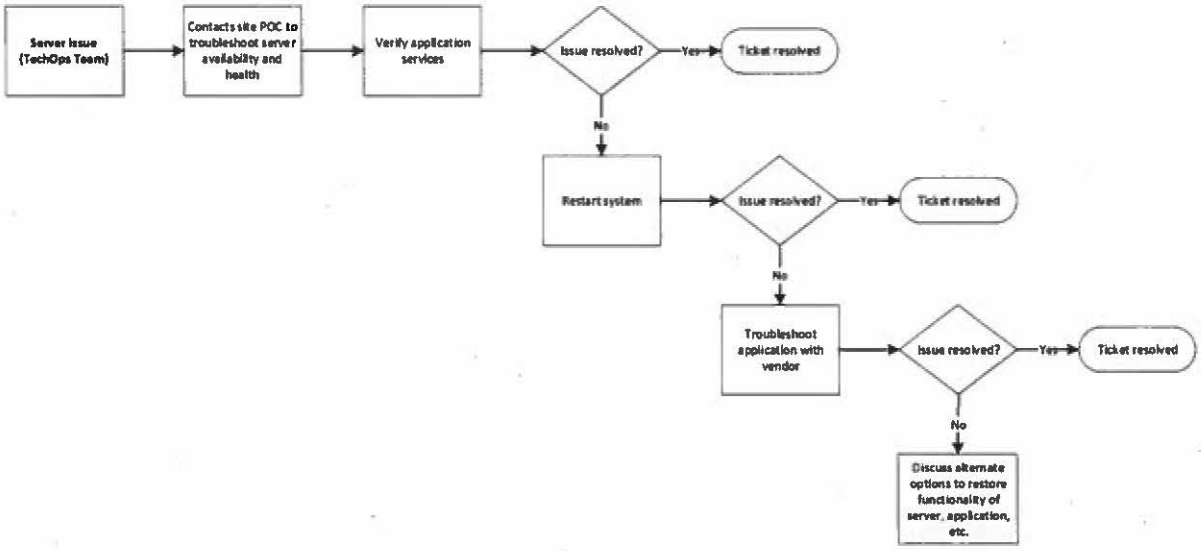
5.4.3.2 Network Issue

If the TechOps Team suspects that the issue is related to a router, switch, etc. they will typically route the ticket to the network team. Below is the workflow demonstrating the troubleshooting steps the network team takes when trying to resolve a network issue.



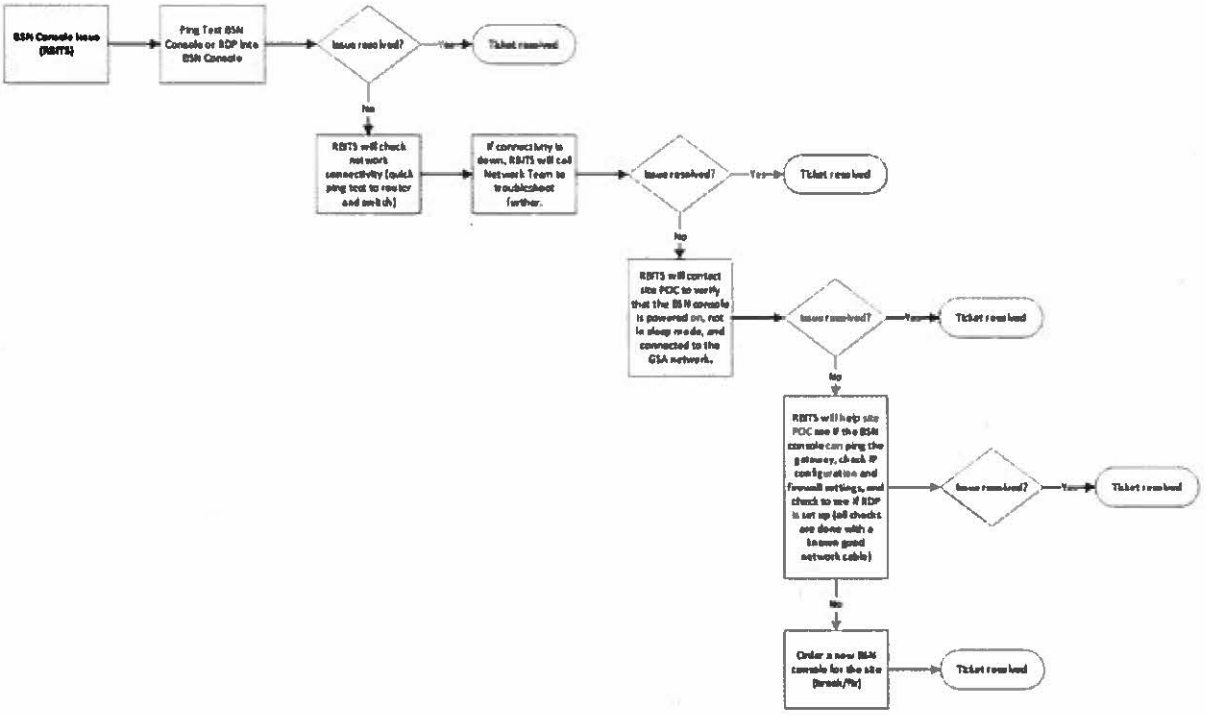
5.4.3.3 BMC Server Issue

As described above in Chapter 5, if TechOps Team suspects that the issue is related to a BMC server, they will continue to troubleshoot the issue. Below is the workflow demonstrating the troubleshooting steps the TechOps Team takes when trying to resolve a server issue.



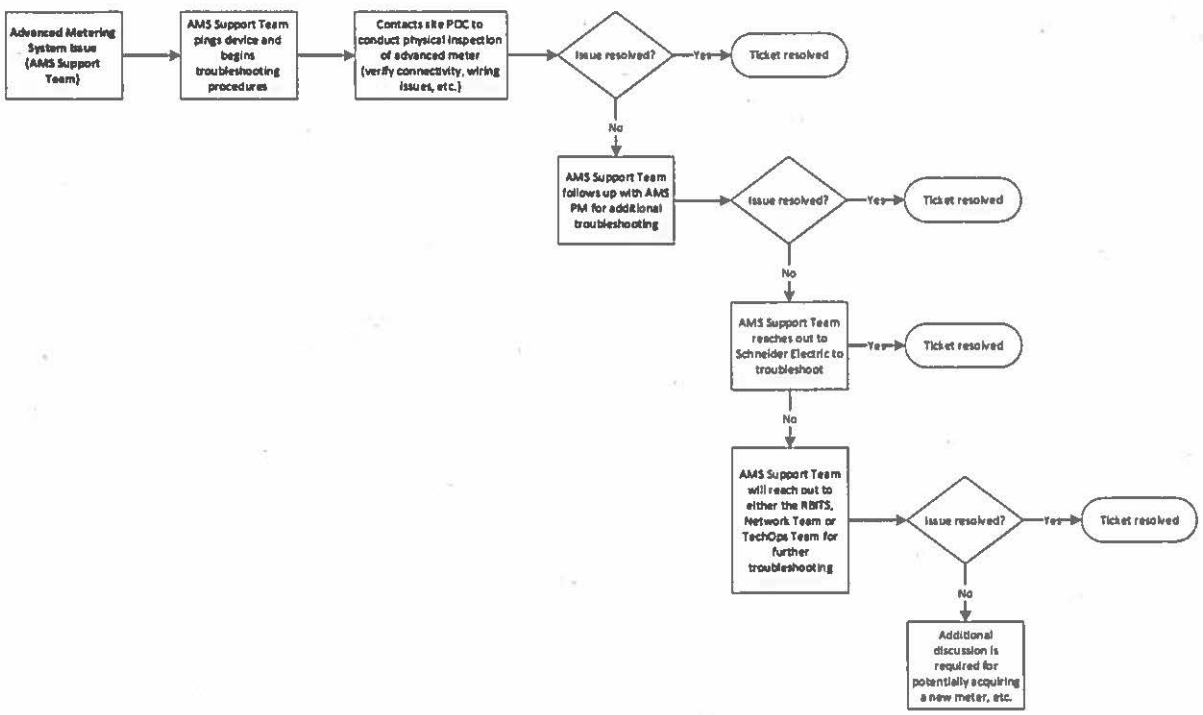
5.4.3.4 BSN Console Issue

If the TechOps Team suspects that the issue is related to a BSN console, they will work in conjunction with the RBITS to troubleshoot the issue. Below is the workflow demonstrating the troubleshooting steps the TechOps Team takes when trying to resolve a BSN console issue.



5.4.3.5 Advanced Metering System (AMS) Issue

Whenever TechOps Team suspects that the issue is related to an advanced metering system, they will typically route the ticket to the advanced metering system (AMS) team in order to further troubleshoot the issue. Below is the workflow demonstrating the troubleshooting steps the AMS team takes in order to resolve the issue.



5.4.3.6 Troubleshooting Points of Contact

Below are the main points of contact for most of the issues stated above. ***Please Note: If an issue needs to be escalated, the caller must indicate that the ticket needs to be assigned a higher priority level.***

- IT Service Desk
  Email: [redacted]
  Phone: 1-866-450-5250
  Hours: Monday – Friday 7 am to 8 pm EST, after hours are by phone call only.

- Network Team
  Email: [redacted]
  Hours: Normal business hours, after hours are by calling IT Service Desk only.

- TechOps Team
  Email: [redacted]
  Phone: 866-274-0781
  Hours: Monday – Friday 7 am to 7 pm EST, after hours are by email only.

- RBITS
  Email: [redacted]
  Hours: Monday – Friday 8 am to 5 pm EST

- AMS Support Team
  Email: [redacted]
  Hours: Normal business hours

Chapter 6

Advanced Metering System (AMS)

6.0 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 470+ facilities.

The platform consists of one enterprise collection server, currently hosting the Schneider ION EEM application, and 10 dedicated regional metering servers (R1, R2, R3, R4, R5, R6, R8, R9 and R10 and NCR), hosting the Schneider Power Metering Expert (PME) application. R7 does not have a PME server but will be migrated to the national platform in early 2021. The 11 servers are managed centrally, as part of the Advanced Metering Systems (AMS) program by GSA-IT. The Schneider metering applications (ION and PME) are 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. ***Please Note: The AMS program may move to a new platform. What is described in this chapter entails the state of the AMS platform as it stands at the time of releasing this version of the BTTRG.***

6.1 Advanced Metering System Roles and Responsibilities

- **Operations and Maintenance (O&M) Support for Advanced Metering System:** The O&M logs and manages all the tickets related to the Advanced Metering Program and they produce the weekly Source Activity Report that provides a count of all down advanced meters across all of 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 update AMS Network diagrams.

- **Schneider-Electric:** Schneider-Electric has a dedicated team of technical support consultants that are responsible for the EEM and PME applications. They provide metering support from the application to the end-user, which includes metering integration, updating network diagrams, source management, etc. They also monitor the Advanced Metering Interface to ensure the system is functioning and they report on system health.

- **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 in compliance 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. Conducts 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 conducts weekly project calls with Redhorse regarding all aspects of metering support. Monitors Uplight (virtual auditing program) reports to trends to ensure that buildings with evaluation requirements have the data needed for evaluations. Coordinate training webinars for end-users and conducts quarterly Metering Network calls with the National/Regional AMS community.

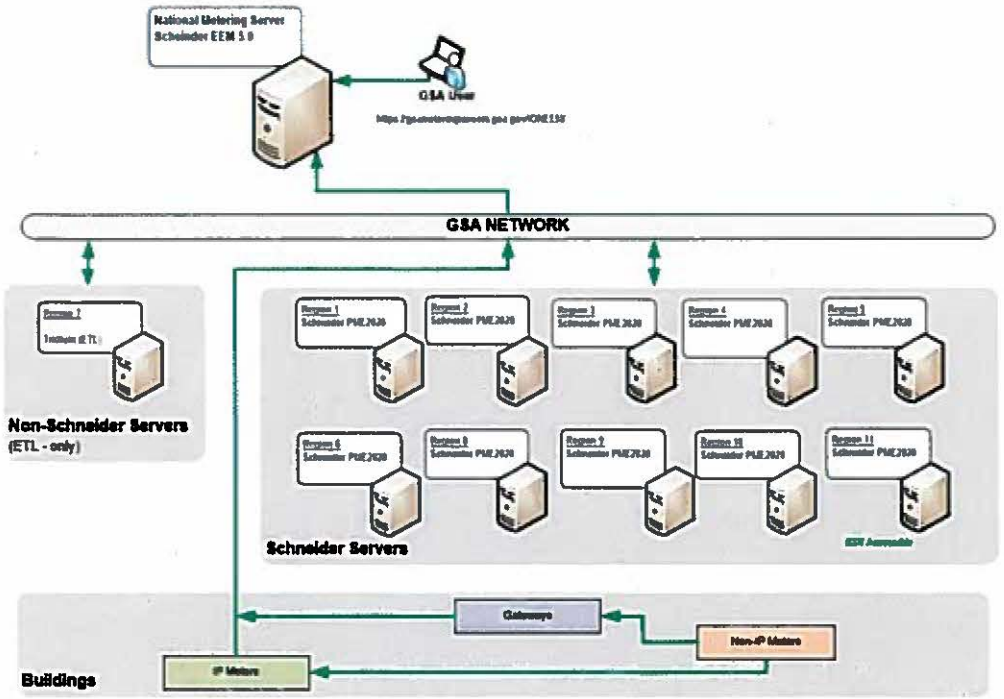
- **Facility Managers/O&M Contractors:** Facility managers/O&M contractors are responsible for confirming meter communication status at their locations and looking at metering data on a regular basis. It's the contractor's responsibility to partner with the GSA to fully utilize the AMS to develop and implement strategies that will result in an overall reduction in energy consumption. The contractor shall 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 (currently ION Enterprise Energy Management). The contractor is also responsible for correcting immediately any onsite communication failure to mitigate any loss of data.

- **Program Lead/Metering Team:** The program lead/metering team 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 and verifying ECM's identified achieve expected energy savings when possible. They also use our data to evaluate building performance for design development and use data post construction to evaluate building performance.

6.2 AMS Architecture

The AMS Architecture, (depicted below) includes 2500 devices, that include IP meters, serial meters (i.e., Modbus), and gateways across 470+ facilities. The majority of the devices report fifteen-minute interval data directly to the corresponding PME server i.e. if the building is in Region 3 the data is recorded on the Region 3 PME server. Subsequently the data is moved to the National Metering server (aka EEM) to provide users with dashboards, reports, and trends. Many devices report data directly to EEM bypassing the mid-tier PME server layer and a couple of regions have proprietary mid-tier servers. Going forward the proprietary servers will be replaced with PME servers and all devices will feed into the mid-tier PME layer.

Advanced Metering Systems Architecture



6.3 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 Device and Application Security Assessment Process.***
- The MAC address for all IP meters must be whitelisted before they can connect to the GSA network. ***Please Note: See Section 1.2.3 for the process of whitelisting devices.***
- All IP meters on the GSA network are subject to continuous monitoring and periodic scanning by GSA-IT.
- All IP ranges/addresses are provided by GSA-IT Network Team, in coordination with the BTDS Technical PM's.

6.4 New Installations

GSA-IT requires PBS to coordinate cabling with a local vendor for completing all runs back to the GSA-provided switches and shall be installed 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. Meters will not be allowed to be integrated into the GSA network with prior approval from GSA-IT. See Section 1.2.3 for details on the BMC Device Whitelisting Process.***

6.5 Support

Reporting an AMS issue using the Advance Metering: Support Request Form [redacted] This form provides information necessary for troubleshooting communication, data loss, or application issues related to advanced metering infrastructure.

6.5.1 Assistance with Support Form

Advanced Metering: Support Request Form

This form provides information necessary for troubleshooting communication, data loss, or application issues related to advanced metering infrastructure. For questions on applicability, or for assistance filling out, please contact [redacted]

The name, username and photo associated with your Google account will be recorded when you upload files and submit this form. Not [redacted] Switch account

* Required

Is this a problem that has been previously reported and has an existing IT ticket number? *

- ○ Yes, and I want to get a status update
- ○ No, this is a new problem

Next

For questions on applicability and assistance with filling out the support form, please contact:

- [redacted]
- [redacted]
- [redacted]

6.5.2 Support Form Questions

- The region associated with the problem.
- Type of problem encountered (i.e., communications, reporting, functionality, other, etc.).
- Building code.
- Is this a meter removal request or a building removal request?
- Regional Main POC.
- Alternative Regional POC.
- Type of Meter (i.e., electric, steam, water etc.).
- Meter Names with problems (metadata meter names found in EEM).
- Meter Model and Manufacturer.
- Total Number of devices affected.
- Building Switch Name (upstream of meter).
- Switch Port Name.
- Device IP or Upstream Device IP.
- MAC Address.
- Is the device Pingable (Y/N?)
- Upload a Network Diagram if available.
- Upload Building Switch Matrix Diagram.
- Upload Pictures of the meters, cables, switches, or other equipment that can help diagnose the problem.
- Approximate start date/time of issue?
- How was the data determined to be incorrect?
- Upload snapshots of Trends that show the error.
- Is this an EEM or PME Problem?
- Any additional information via freeform description?

6.5.3 Post-Support Form Process

- The questionnaire above must be answered by Regional POCs/O&M Tech in order to generate a ServiceNow Incident or Catalog Request and to avoid any unnecessary delays in supporting AMS.
- All pertinent information from the support form is copied to the ServiceNow ticket by the AMS Support Team.
- AMS Support Team will generate a ServiceNow Incident or Catalog Request using the responses from questions.
- AMS Support Team will use the information from the support form to create a ServiceNow ticket that is managed through the AMS Support Workflow.
- Connectivity issues - After a failed ping, AMS Support Team may arrange a physical inspection of the device with the help of the Regional POC/O&M Tech.
- The support team will reach out to the RBITS through the BTSD Technical PM.
- Depending on the initial diagnosis, AMS Support Team may escalate the issue to the TechOps/network team and or engage the vendor if necessary.
- If necessary, a child ticket is generated for other technical support teams such as TechOps and or the network team.
- Tickets will be resolved by the AMS Support Team when an agreeable solution is provided for the AMS issue.
- Tickets are automatically closed 7 days after a ServiceNow ticket status is changed from Open/work in progress/pending to Resolved.

6.6 Metering Issues

If the AMS Support Team is directly contacted for a technical issue, they will create an incident ticket in ServiceNow. The AMS O&M Support Team will work with TechOps to direct incidents through the proper channels and assign them to specific resolution groups. They work with O&M contractors, facility manager, and regional metering POCs to coordinate on-site triage. They also work with the metering vendors for full implementation of communication restoration. The AMS Support Team also runs the Source Activity Report on a weekly basis to identify meters that are not working.

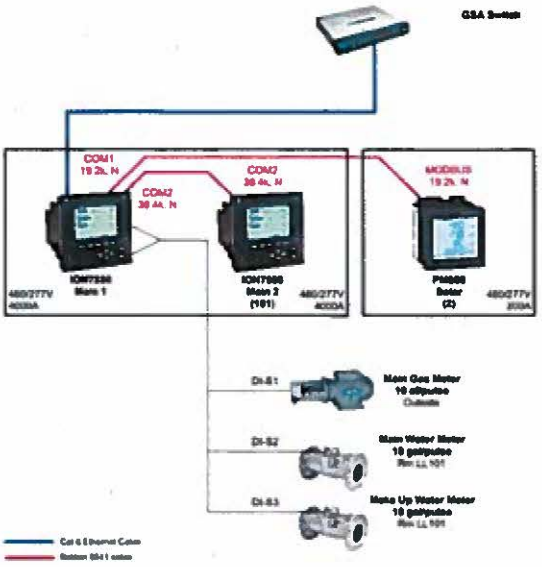
As the AMS Support Team troubleshoots the ticket, it will determine which GSA-IT service organization or BMC vendor is best positioned to resolve the problem. When a problem arises, the person reporting the problem completes the Advanced Metering: Support Request Form as described in section 6.5.1 of this document. The AMS Support Team then creates an incident ticket in ServiceNow.

The AMS Support Team then begins the process by pinging the device and checking its status on SolarWinds to verify connectivity. The Site POC may be contacted as well to conduct a physical inspection. On occasion, the AMS Support Team reaches out to the BTSD team as well to confirm if there were changes or updates to the network at the site in question.

Lastly if the device is physically intact and operating, the AMS Support Team will, then validate if the problem is server based, network based, or application based. The ticket will then be routed to the appropriate team (i.e., TechOps, network team or Schneider Electric). ***Please Note: An Advanced Metering Support Workflow can be found in Chapter 5, section 5.4.3.5.***

6.7 Sample Network Diagram

Riser 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: See Section 2.4.2 for a sample network riser diagram that needs to be submitted for all new metering integrations.***



Chapter 7

Physical Access Control System (PACS)

7.0 Overview

This chapter will provide guidance on access management tools being utilized by GSA for GSA-controlled space leveraging the GSA-IT infrastructure. A system composed of hardware and software components that control 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 in order to gain entrance into secured areas.

Most compromises to the GSA network originate from within GSA (ENT) networks as a result 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 (personally identifiable information (PII)) potentially accessible via PACS, requires a more robust approach to security than currently required with other Building System Controls. To this effect, a dedicated chapter was developed for these systems.

7.1 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 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 server (physical or virtual) supplied by TechOps for any initiative related to a PACS deployment per their normal Standard Operating Procedures (SOP) and support guidelines. Please contact: [redacted]

- **GSA-IT Building Technologies Service Division (BTSD):** The BTSD team's roles and responsibilities related to PACS, will vary from those outlined within this guide for other Building System Controls. BTSD will work in conjunction with The Office of Mission Assurance (OMA), GSA-IT and PBS. BTSD will provide assistance with the network infrastructure, authorize and issue IP addresses, submit MAC whitelisting requests (after provided by OMA) and 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 System 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.

- **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. All GSA related PACS projects and/or space within the GSA inventory must be fully compliant with HSPD-12, FIPS201, and Federal Identity, Credential and Access Management (FICAM) standards. Therefore, all GSA projects will follow the *National Scope of Work (SOW) for PACS Integration/ Migration* and will adhere to *GSA Order 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. As noted in Section 7.3.1 of this document, OMA will provide guidance on the procurement, implementation, administration and oversight for physical security countermeasures (aka "fixtures") as outlined in the *2018 DHS - GSA MOA*. Regarding O&M of PACS, OMA will work with GSA-IT and PBS to 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.

7.2 Security

All PACS devices that will be used on the GSA network will be evaluated by the BMC-IT Security. 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 *IT Security Procedural Guide: BMC DEVICE ASSESSMENTS.* For a copy of this document, please email [redacted]

The project activities performed by the BMC-IT Security team in supporting this program include, but are not limited to, the activities described below. The BMC-IT Security team reviews program manager submissions and evidence, conducts independent testing, and documents all findings. The BMC-IT Security team facilitates the development of and performs documentation review of articles which include vulnerability scan results and the Security Assessment Report (SAR).

The BMC-IT Security team then develops reports and other required documents to complete the security function. The team then provides guidance to the OMA Program Manager to remediate all findings listed in the SAR.

Specific Security Requirements for GSA PACS Systems:

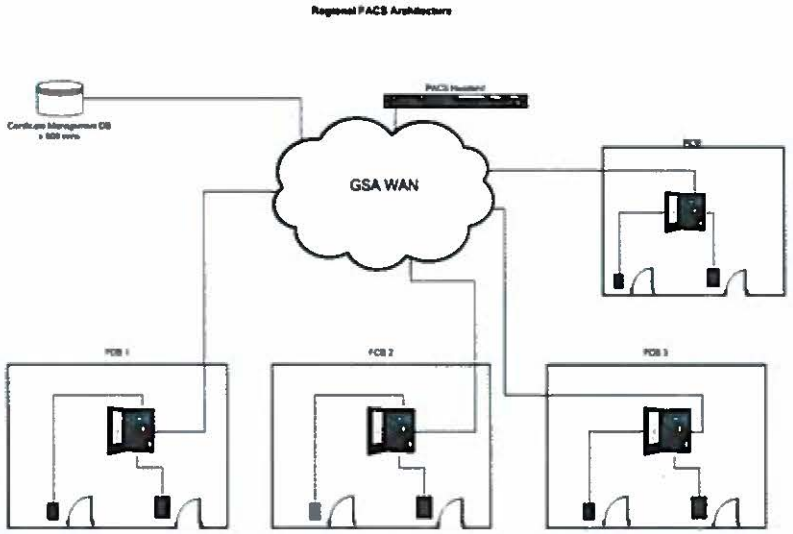
- All PACS devices that will be implemented on the GSA network must adhere to current [redacted]

- 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.

7.3 PACS Architecture and Integration

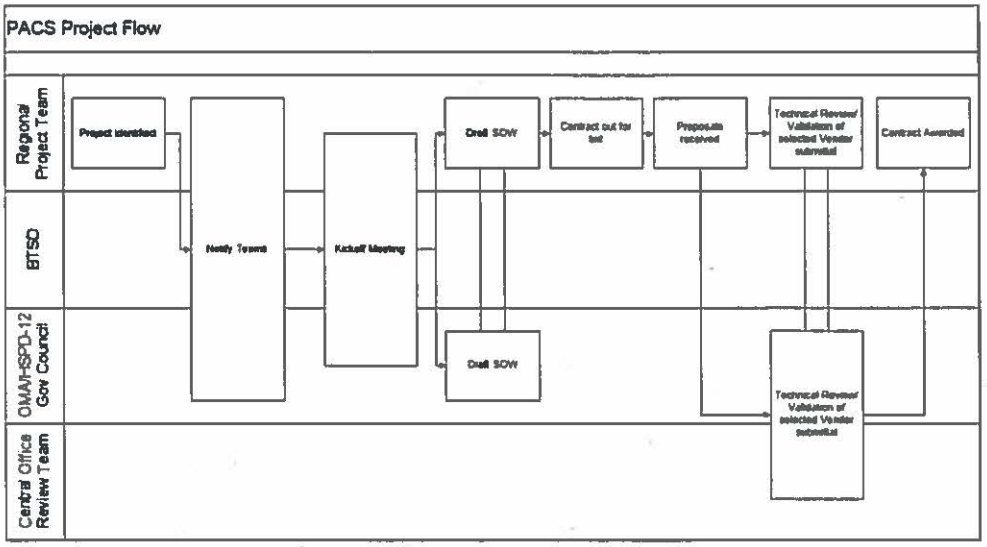
The PACS network architecture consists of a centralized appliance/headend and centralized certificate management piece that each Field Office Building (FOB) connects to and is integrated with. All PACS projects and integrations must meet current GSA, GSA-IT, OMA policies, and other applicable Federal 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 devices as well as the centralized headend and certificate management devices. ***Please Note: Head-end refers to a server-based system or appliance-based system that pushes settings down to the respective readers/panels.***

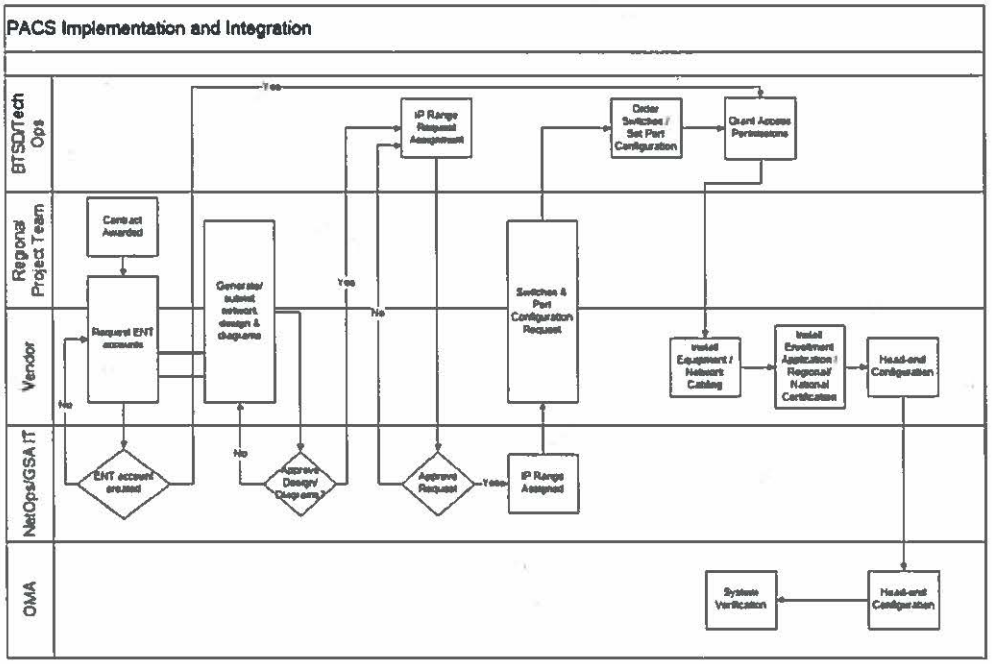
The following diagram provides the layout for the regional network architect:



7.4 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 BMC-IT Security.***





7.5 Support

Trouble 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 related issues. ***Please Note: See Section 5.4 for details on how to report a BMC issue.***

Chapter 8

BMC Procurement: IT Requirements in Scope of Work (SOW)

8.0 Overview

This chapter entails recommended 'scope of work' content 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).

8.1 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. Background

   In recent years, building systems have advanced to more closely resemble 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 General Services Administration (GSA) Public Building Services (PBS) Building Information or Control System Technology Policy mandates that all building technologies which require network or internet connectivity must utilize the GSA network. GSA's Public Buildings Services' (PBS) Office of Facilities Management (OFM), 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 controllers and End of Life (EOL) components.
   - Improve accessibility to operational and energy data.
   - Leverage IT infrastructure to improve BMC reliability and performance.

2. 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. General Scope

- Replace all ten (10) Level-3 (Automation IP Level) Global Network Controllers (GNC) and applicable I/O, protocol port, or add-on modules with new GNCs. Upgrade shall include the database, modules, licenses, programming, graphics, etc. be upgraded to the latest PB-ITS remediated version of the manufacturer software.
- 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 five-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 five-year period.

4. 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. Required IT Security Documents

- Building Technologies Technical Reference Guidelines (latest version posted on [redacted]
- Telecommunications Distribution Design Guide (latest version posted on [redacted]
- CIO-IT Security-16-76 IT Security Procedural Guide Building Monitoring and Control (BMC) Systems Security Assessment Process (latest version posted by on [redacted]
- CIO-IT Security-09-43 IT Security Procedural Guide: Key Management (latest version posted by on [redacted]
- GSA Order CIO 2100.1 Information Technology (IT) Security Policy (latest version posted on [redacted]
- CIO-IT Security-06-30 IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk (latest version posted by on [redacted]
- GSA order CIO P 2181.2 GSA Rules of Behavior for Handling Personally Identifiable Information (PII) (latest version posted by on [redacted]

- 2181.1 ADM Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors (latest version posted by on [redacted]
- 2180.2 CIO GSA Rules of Behavior for Handling Personally Identifiable Information (PII) (latest version posted by on [redacted]
- 2100.2B CIO P GSA Wireless Local Area Network (LAN) Security (latest version posted by on [redacted]
- CIO 12-2018, IT Policy Requirements Guide (latest version posted by on [redacted]
- CIO 09-48, IT Security Procedural Guide: Security and Privacy IT Acquisition Requirements (latest version posted on [redacted]
- [redacted]
- [redacted]

6. 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. 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%.

- **Security:** 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 I clearance, which is a prerequisite to acquiring ENT (GSA user domain) credentials, necessary to access any GSA furnished workstation or server.

    - Per GSA CIO policy 2100.1, 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.

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

    - 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.

    - Contractor is responsible for maintaining ENT accounts for all its employees. This includes logging into account regularly, changing ENT passwords every 90 day, 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.

- **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. ***Please Note: See Chapters 2 and 3 for details on basic cabling information.***

- **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. 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 in order 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. Vendor provided diagrams must be submitted in digital display in Microsoft Visio.

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

- A proposed network diagram of all IP addressable devices that terminate on the GSA network shall be provided to the BTSD Technical PM/RBITS. The GSA-IT shall be included in the design phase of the network infrastructure. Vendor provided diagrams must be submitted in digital display and in an editable format, such as Microsoft Visio.

- Any contractor-provided hardware/controllers/applications requiring access to the GSA network must comply with GSA-IT security requirements.

- All IP enabled devices will be evaluated and scanned 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 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 outcome with respect to meeting the established security requirements. The 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 aforementioned 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 server for application 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 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.
- 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. In order 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] or 866-450-5250). An Incident is a violation or an imminent threat of violation of information security or privacy policies, acceptable use policies, or standard security practices. For questions about GSA's Incident Response Program, contact the GSA Incident Response Team at [redacted]

- 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 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.

- 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.

- 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.

- 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 BMS contractor shall coordinate a date to "Cut-Over," the BMS system from the existing server and onto the new BMS Server. The BMS 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 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. 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 coordinated through the GSA Facility Management team at the building.
- Upgrades shall be performed within timeframes agreeable to GSA in order to mitigate risk and/or downtime to the GSA facility.

10. 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. 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.

Chapter 9

Best Practices for BMC Systems Project Implementations

9.0 Overview

This chapter entails best practices for integration of BMC systems to the GSA network. In this iteration of the guide, a commissioning/project cutover checklist has also been added.

9.1 Tips for Running a Successful BMC 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, network and connectivity requirements. Potential Stakeholders include:
  - BTSD Technical 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 the procurements. ***Please Note: See Section 8.1 for more details.***
  - ***Per the P100, Chapter 7 - Fire Alarm and Emergency Communication Systems: "With the exception of 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.

- 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
  - 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 consult 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 five-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 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 in order 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.

9.2 BMC 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.

9.2.1 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 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.

9.2.2 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 Server.
- The Alarm Recipient (Server) shall route alarms properly.
- AMS points are required to be shared from the BMC global controller metering graphic page.
- AMS points are required to be mapped to AMS Server.

9.2.3 General Documentation and Deliverables

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

9.2.4 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 Sensitive But Unclassified (SBU) information. All SBU information must use secure transmission channels, and by using GSA.gov domain email address.

Appendix

Appendix A: Contact Information

Team/Division	Contact Information
Buildings Technology Services Division	[redacted]
PB-ITS Technical PMs	[redacted]
Regional Building IT Specialists	[redacted]
GSA-IT BMC Security	[redacted]
Technical Operations Team	[redacted] 866-274-0781
Network Team	[redacted]
Security Operations	[redacted]
Advanced Metering System Support Team	[redacted]
Requirements Analysis Team	[redacted]
HSPD-12 Credentialing Questions	[redacted]
GSA-IT Service Desk	[redacted] 866-450-5250

Appendix B: Listing of Reference Policies

Item	Guide/Document Name	Description/Link
B.1	FIPS 140-3	Federal Information Processing Standard (FIPS) is a certification that specifies the exact module name, hardware, software, firmware, and/or applet version numbers. Encryption is an important tool used to meet security control requirements. When used to protect sensitive information Federal systems must use encryption that meets the requirements of the Federal Information Processing Standard (FIPS) 140-3. 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. The National Institute of Standards and Technology (NIST) promulgated FIPS 140-3 to ensure that encryption technology meets minimum standards when protecting sensitive data on Federal networks and systems. All cryptographic modules used in Federal systems must meet the standards in FIPS 140-3. FIPS 140-3 provides a certification path for vendors of cryptographic modules. Certification ensures that the standards are met in the specific vendor implementation. Wireless and SFTP (Secure File Transfer Protocol) Data Transmissions also need to meet FIPS 140-3 protocol. [redacted]

B.2	CIO-IT Security-16-76 IT Security Procedural Guide: Building Monitoring and Control (BMC) Systems Security Assessment Process	[redacted] (search for latest version on InSite). Version2 was the latest published version available during the release of this guide.
B.3	CIO-IT Security-09-43 IT Security Procedural Guide: Key Management	[redacted] (search for latest version on InSite). Version 4 was the latest published version available during the release of this guide.
B.4	GSA Order CIO 2100.1L Information Technology (IT) Security Policy	[redacted] (search for latest version on InSite). Version 2100.1L CHG 1, was the latest published version available during the release of this guide.
B.5	CIO-IT Security-06-30 IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk	[redacted] (search for latest version on InSite). Version 18 was the latest published version available during the release of this guide.
	2100.2B CIO P GSA Wireless Local Area Network (LAN) Security	[redacted]
B.6	2180.2 CIO GSA Rules of Behavior for Handling Personally Identifiable Information (PII)	[redacted]
B.7	CIO Order ADM 2181.1 Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors	[redacted]
B.8	Access Card Policy and Guidance Resources	[redacted]
B.9	NIST 800-82 rev 2	[redacted]
B.10	NIST 800-53 rev 5	[redacted]

Appendix C: Change Log

Revision	Chapter	Change
Revision 1.1	1	TIC
	1	Formal Security Evaluation

Revision	Chapter	Change
	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
	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

Revision	Chapter	Change
	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 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

Revision	Chapter	Change
	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)"
	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"

Revision	Chapter	Change
	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)
	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"

Revision	Chapter	Change
	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"
	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"

Revision	Chapter	Change
	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"
	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"

Revision	Chapter	Change
	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"
	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"

Revision	Chapter	Change
	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't 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 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"

Revision	Chapter	Change
	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
	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

Revision	Chapter	Change
	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"
	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"

Revision	Chapter	Change
	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"
	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"

Revision	Chapter	Change
	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