# IT Security Procedural Guide: Building Monitoring and Control (BMC) Systems Security Assessment Process CIO-IT Security-16-76

**Revision 4**

March 25, 2024

Controlled by: General Services Administration
OCISO ISP Division: ispcompliance@gsa.gov

*Office of the Chief Information Security Officer*

# VERSION HISTORY/CHANGE RECORD

| Change Number | Person Posting Change | Change | Reason for Change | Page Number of Change |
|---|---|---|---|---|
| | | **Initial Release – August 24, 2016** | | |
| 1 | Jaworski | Initial development of BMC assessment procedures | Standardization of BMC device assessments | All |
| | | **Revision 1 – August 29, 2018** | | |
| 1 | Smith | Updates made throughout document | Updates made to address new RMF process | All |
| 2 | Feliksa/ Dean | Edited and revised structure and format | Technical editing, update to standard structure and format | All |
| | | **Revision 2 – October 1, 2020** | | |
| 1 | Fisher | Updates include:<br>• Updated guide to use the term Building Monitoring and Control (BMC)<br>• Created a graphic of the BMC assessment process<br>• Updated step tables and tied them to the process graphic using header colors<br>• Refined the processes and templates used for assessments<br>• Updated to current style/format for guides | Biennial update | All |
| | | **Revision 3 – March 25, 2024** | | |
| 1 | Fisher | Updated:<br>• GSA IT Security policy and best practices<br>• Wireless Security requirements<br>• IPv6 requirements<br>• Windows/Linux patching<br>• BACnet SC<br>• Network Topology diagram | Periodic update | All |
| 2 | McCormick | • Moved Executive Summary to improve information flow<br>• Edited to align with current GSA documentation guidelines<br>• Added CUI Marking based on Figure 3-1 | | All |
| | | **Revision 3 – March 25, 2024** | | |
| 1 | Klemens, Fisher | Added reference, requirements, and other information related to the IoT Cybersecurity Act of 2020. | Align with the IoT Act. | 2, 13, 16, 21, Appendix C |

# Approval

IT Security Procedural Guide: Building Monitoring and Control (BMC) Systems Security Assessment Process, CIO-IT Security 16-76, Revision 4, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas
Chief Information Security Officer

DocuSigned by:
Philip Klokis
6F8E4C8418E2469...

Philip Klokis
Associate Chief Information Officer (IP)

**Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.**

# Table of Contents

# 1 Executive Summary

This guide establishes standard processes and procedures for evaluating the Information Technology (IT) security of a submitted Building Monitoring and Control (BMC) Systems component for approved initial use by the General Services Administration (GSA) Public Building Service (PBS). BMC components encompass BMC devices and Supervisory Control Software (SCS). These processes should not be used in place of the approved Federal Information Security Modernization Act (FISMA) review process for the Building Services Network (BSN) at GSA. This guide formalizes the workflow, provides associated time frames for each process step, and establishes the criteria used to identify the risk posture presented by BMC system components within the PBS environment. The test procedures can be used to supplement the approved FISMA review process.

Participation and timely responses from BMC Vendors, the BMC Assessment Team, the Building Technology Services (BTS) Division under the Public Buildings Information Technology Services (PB-ITS), and other BMC Stakeholders are essential for a successful BMC system component assessment. This guide documents the current practices used in the BMC Assessment Lab. GSA IT realizes that as the BMC industry matures and more stringent hardening and security requirements are implemented, this process will adapt to the changing environment. This guide will be reviewed and updated to reflect any change in processes, as necessary. This guide identifies six essential process steps in reviewing the risk posture of each BMC component submitted to the BMC Assessment Lab. Details of each step are provided in Figure ES-1.

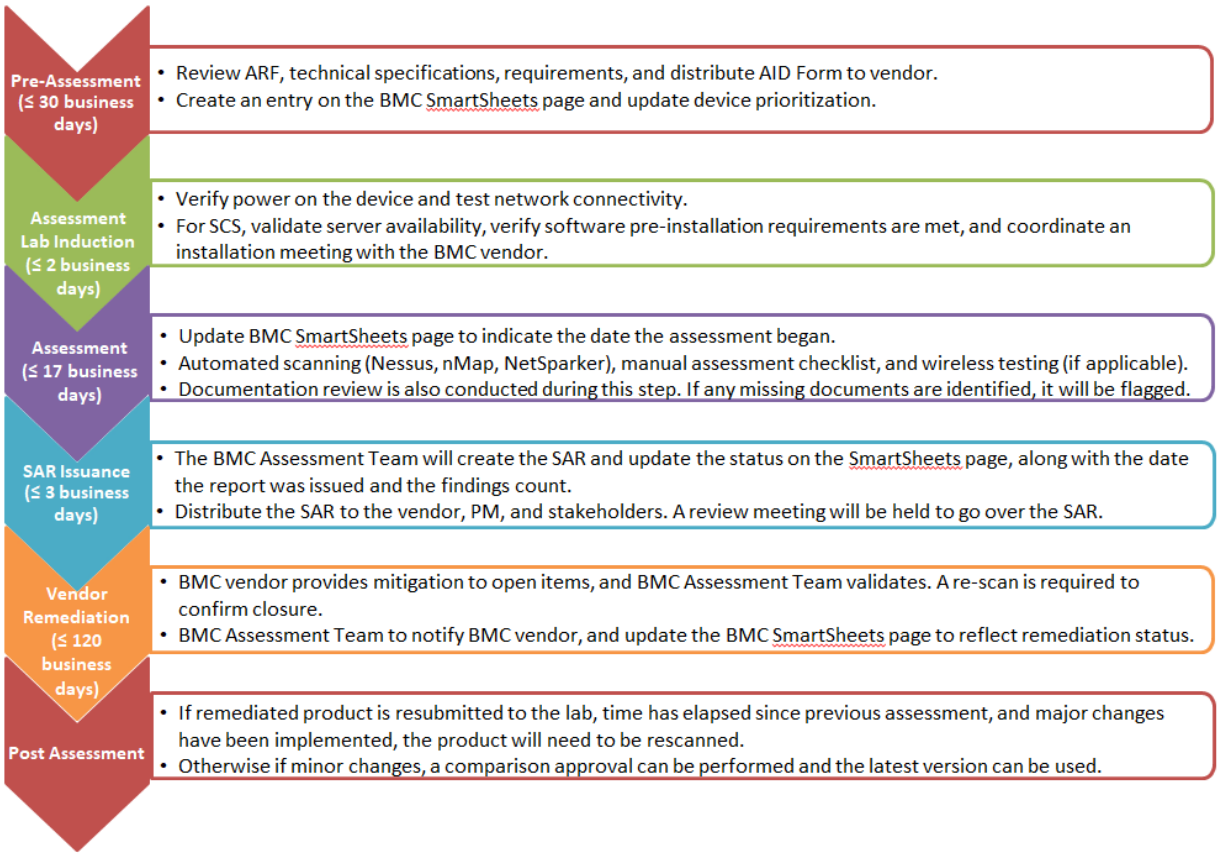


**Figure 1-1: Six Essential Steps for BMC Component Assessment**

# 2 Introduction

BMC solutions are a subset of Operational Technology (OT) which support building automation and centralized control through the ability to logically and physically connect BMC components to traditional IT networks. BMC devices can be managed via an SCS or can operate independently. BMC includes Internet of Things (IoT) as devices that have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world.

As the OT/IoT field is a maturing discipline, GSA recognizes that not all BMC solutions meet the requirements typically incorporated into mainstream IT hardware and software products. However, to achieve GSA's mission and to meet GSA customer needs, the GSA Office of the Chief Information Security Officer (OCISO) has established the following process for evaluating the IT security risk posture of BMC solutions proposed for use within GSA-owned facilities.

## 2.1 Purpose

This guide defines the procedures for assessing BMC solutions submitted to the GSA OCISO by the Public Building-Information Technology (PB-ITS) Building Technology Services (BTS) Division. This process is designed to ensure that a reasonable level of due diligence is performed through an initial security evaluation of each BMC solution's technical, operational, and management capabilities, such that the BMC solution's vulnerabilities are identified and remediated prior to the solution's installation into GSA IT network environments. This document also formalizes the workflow and associated time frames for each step in the process.

## 2.2 Policy and Guides

GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy," states in:

Chapter 3, Policy for Identify Function, Section 6, Supply Chain Risk Management:

*g. Internet of Things (IoT) devices cannot be procured unless a review of the contract by the CIO identifies that it complies with NIST SP 800-213 or the CIO grants a waiver under one of the conditions of the IoT Act. Any waivers must include the elements identified in the IoT Act and be sent to the GSA Administrator.*

Chapter 5, Policy for Detect Function, Section 2, Security Continuous Monitoring:

*t. Systems will be scanned for vulnerabilities of operating systems and web applications periodically IAW GSA CIO-IT Security-17-80: Vulnerability Management Process. Vulnerabilities identified must be remediated IAW GSA CIO-IT Security-06-30: Managing Enterprise Risk.*

The PB-ITS Building Technologies Technical Reference Guide, states in Chapter 1, Paragraph 1.3.3:

> *All IP addressable devices, appliances or servers that will communicate over the GSA network must be scanned by GSA-IT Security. Before any hardware, software or IT device/system is connected to its network, a security risk assessment of selected management, operational, and technical security controls is performed to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. A security assessment report is produced by GSA IT Security once the device*

*has been assessed, which will be provided to the BMC stakeholders and the vendor. The assessment report will allow GSA to understand and accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals Based on the implementation of an agreed-upon set of security controls. The contractor/vendor must therefore be held responsible for mitigating all security risks identified. Vulnerabilities must be mitigated within the appropriate timeframe as described in the Security Assessment Report mitigation plan along with milestones and timelines for remediation for consideration of GSA-IT in order to connect to the GSA network. GSA IT only needs to scan a certain model device once and not for each project. Once the device has completely gone through the remediation process and has a remediation/hardening plan in place, all other projects can use that report to configure the named device accordingly.*

# 3 BMC Security Assessment Process

The following sections describe the major steps and significant sub-components involved in the BMC Security Assessment Process. Each step includes a corresponding table (with the table header color-coded to match the steps described in Figure 1-1). Each table indicates responsibilities, expectations, and expected response time to complete each step. The response time documented is solely based on time to complete the task and does not take into consideration the time to troubleshoot issues or gather missing requirements. Any issues increase the delivery and/or response time for each step.

**Note:** An assessment is conducted only for BMC solutions already under an existing GSA project. There is no pre-assessment of BMC solutions prior to contract award. Furthermore, each BMC component submitted to the lab must have an assigned project sponsor who must provide information on the current project plan to implement the device/application.

Smartsheet is used to track the project development and workflow for all BMC solution assessment projects. A status update on BMC solution assessments is provided to the BTS Division weekly and communicated to other stakeholders as needed.

## 3.1 Step 1: BMC Pre-Assessment

The BTS Division is responsible for working with BMC Vendors to identify BMC solutions needing assessment. During this stage, the BTS Division collaborates 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. Table 3-1 summarizes the responsibilities, expectations, and tracking of Step 1, BMC Pre-Assessment.

**Table 3-1: BMC Pre-Assessment**

| Step 1 | Responsibilities, Expectations, and Tracking for BMC Pre-Assessment |
|---|---|
| **Responsible Role(s)** | **BTS Division, PBS project Stakeholders, Vendor, BMC Assessment Team** |
| Internal Tracking Requirement | 1. Review BMC ARF and corresponding information.<br>2. Validate technical specifications and requirements. |

| Step 1 | Responsibilities, Expectations, and Tracking for BMC Pre-Assessment |
|---|---|
| | 3. Create an entry in Smartsheet if all pre-assessment requirements are met and determine risk level.<br>4. Distribute BMC Assessment Identification Form<br>5. Identify and update device prioritization |
| Expected Response Time | ≤ 30 business days<br>**Note:** BMC Assessment Lab acceptance response time is dependent upon the timeliness and quality of vendor documentation delivery, the BTS Division response time, and BMC Stakeholder prioritization process. |

### 3.1.1 BMC Security Assessment Request Form

Completing the BMC Security Assessment Request Form (ARF) is the first requirement in the pre-assessment phase. The form must be submitted to the BMC Assessment Lab prior to shipping the device or installing the software. This form provides the additional details and configuration information required to complete the device assessments. Failure to provide these additional details could result in a delay and/or rejection of an assessment.

Completion of the BMC ARF includes the following:

- BMC ARF (Required)
  - See Appendix A for a link providing access to the BMC ARF (Google Form) located within the GSA's InSite (Intranet).
    - If unable to access GSA's InSite page, utilize the latest version of the ARF Checklist Spreadsheet provided by a GSA Point of Contact (POC).
  - The BMC ARF must be completed by the BMC Sponsor and/or a BMC project POC before the device is shipped to, or software is installed in, the BMC Assessment Lab.
  - All required fields, identified with an asterisk "*" must be completed to submit the final form.
  - Prior to submitting the form, upload all files associated with the software or device to the link provided in the ARF.
  - Note: Responses that provide more complete information and details will lead to a more thorough and timely assessment.
- ARF Checklist Spreadsheet (Required for vendors who cannot access GSA InSite (intranet))
  - The ARF Checklist Spreadsheet is provided to the vendor by the Project Manager (PM) for information collection. The ARF Checklist Spreadsheet enables data gathering from vendors who cannot access the GSA Google Tools and Drives. The ARF Checklist Spreadsheet is identical to the BMC ARF, making data input into the BMC ARF easier for PMs.
  - Any sensitive information being collected in this process should be handled with care and appropriate security steps used, such as GSA-approved file encryption.
  - Prior to sharing the ARF Checklist Spreadsheet, all files associated with the software or device must be included along with the ARF Checklist Spreadsheet.
  - Note: responses that provide more complete information and details will lead to a more thorough and timely assessment.

- A link to the latest version of the ARF Checklist Spreadsheet can be found at Appendix A.

### 3.1.2 BMC Documentation Verification and Review

All BMC device and SCS requests must be accompanied by system documentation commensurate with their functionality. This documentation should be submitted through the BMC ARF mentioned above. Typical documentation examples include:

1. Overview of management software functionality and capabilities.
2. Network diagram detailing network ports, protocols, and services utilized for communication between the BMC Vendor's management software device, including management or metering equipment. Any connection established outside the building network should be identified. Any wireless technology request should include the following information: Federal Communications Commission (FCC) ID, protocol specification, operational documentation, commissioning guides, and any standard accreditation documents (e.g., Zigbee Alliance accreditation).
3. Operation & Maintenance guide(s) for all the hardware, firmware, and software submitted for assessment. Note that this must include the BMC Vendor's life cycle support schedule and service agreement for hardware, firmware, and software updates due to identified security vulnerabilities.
4. User Guide(s) for all the software submitted for assessment, any end-user licensing agreements, and supporting patch management processes.
5. Security Configuration Guide(s) for all hardware and software submitted for assessment.
6. Any additional specifications or requirements for the use of wireless technologies or other standards and protocols used.

The BMC Assessment Team is responsible for the initial review of the documentation provided through the BMC ARF. If the Assessor identifies missing items or gaps in documentation, a notification is sent to the BMC Vendor, BTS Division PM, and BMC Stakeholder. If the additional documentation is not provided within 21 calendar days, the assessment will not have enough supporting evidence to continue and the BMC Assessment Team has the right to close the assessment. The BMC Smartsheet page is updated to reflect the lack of information and the assessment identified as closed.

### 3.1.3 BMC Technical Prerequisites and Review

The BMC device must be submitted to the BMC Assessment Lab in a state to utilize power from a standard 110V wall outlet. The BMC Assessment Team is NOT permitted to work with any electrical wiring, and any device that cannot immediately be plugged into an 110V wall outlet will be delayed. Additionally, if the device requires a functioning Power over Ethernet (PoE) adapter, the PoE requirements must be documented in the BMC ARF. If the BMC Assessor is unable to power the device, it is either returned for proper configuration, or the BMC Device assessment is placed on hold until the BMC Vendor support can configure it appropriately in the BMC Assessment Lab. All SCS requests should be submitted with all necessary installation files, an activation license file, and a technical POC to assist in software installation. If the properly configured devices or software files are not provided within 21 calendar days, the BMC Assessment Team has the right to close the assessment. The BMC Smartsheet page is updated to reflect the configuration deficiency and the assessment is marked as closed.

The BMC device must be submitted to the BMC Assessment Lab configured and hardened, as it will be installed on the GSA network (unnecessary ports and services closed, etc.). If the BMC device is submitted with the following configurations, it is immediately rejected without further review. The BMC Smartsheet page is updated to identify the technical deficiency and the assessment is closed.

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

- Remote Access (back doors) from outside of the GSA network. Access must use GSA-provided access (Citrix, Virtual Desktop Interface [VDI], or Government Furnished Equipment [GFE] with Virtual Private Network [VPN]).
- Use of third-party providers (cloud, hosting, etc.) is restricted to only GSA-approved and FISMA reviewed third party providers.
- Protocols such as Telnet, Secure Shell (SSH), Trivial File Transfer Protocol (TFTP), FTP, and Hypertext Transfer Protocol (HTTP), are not accepted due to the unencrypted nature of the protocols.
- The BMC Device must not allow changes to security configuration without authentication.
- The BMC Device must not have hardcoded credentials.
- Use of compromised or weak wireless technology, such as Zigbee (default configuration without any modification), Z-Wave (default configuration without any modification), Bluetooth, Institute of Electrical and Electronics Engineers (IEEE) 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).
- Building Automation and Control Networks (BACnet) are reviewed on a case-by-case basis.
    - BACnet/Ethernet- Because Layer 2 network traffic cannot be effectively managed on the GSA network between subnets, BACnet/Ethernet is expressly prohibited from being implemented on the GSA Wide Area Network (WAN). BACnet/Ethernet can be used at a given field site, provided all BACnet devices are on the same subnet.
    - BACnet/Internet Protocol (IP) Multicast (B/IP-M) - BACnet multicasting is another way to communicate BACnet messages from one subnet or broadcast domain to another. However, GSA does not allow multicasting over its WAN. Therefore, this approach should not be applied when configuring a BACnet system on the GSA network.
- Windows and Linux based controllers not capable of compliance hardening and monthly OS patching.
- Not IPv6 capable when connected directly to the GSA switch.
- Server software incapable of utilizing Windows Server 2022.
- BSN console software incapable of utilizing Windows 11.

Figure 3-1 shows the approved network topologies that are allowed on the BSN or ENT. Any other connections/topologies are not allowed. ***Please Note: The gray circled scenarios can be approved by BMC-IT Security on a case-by-case basis.***

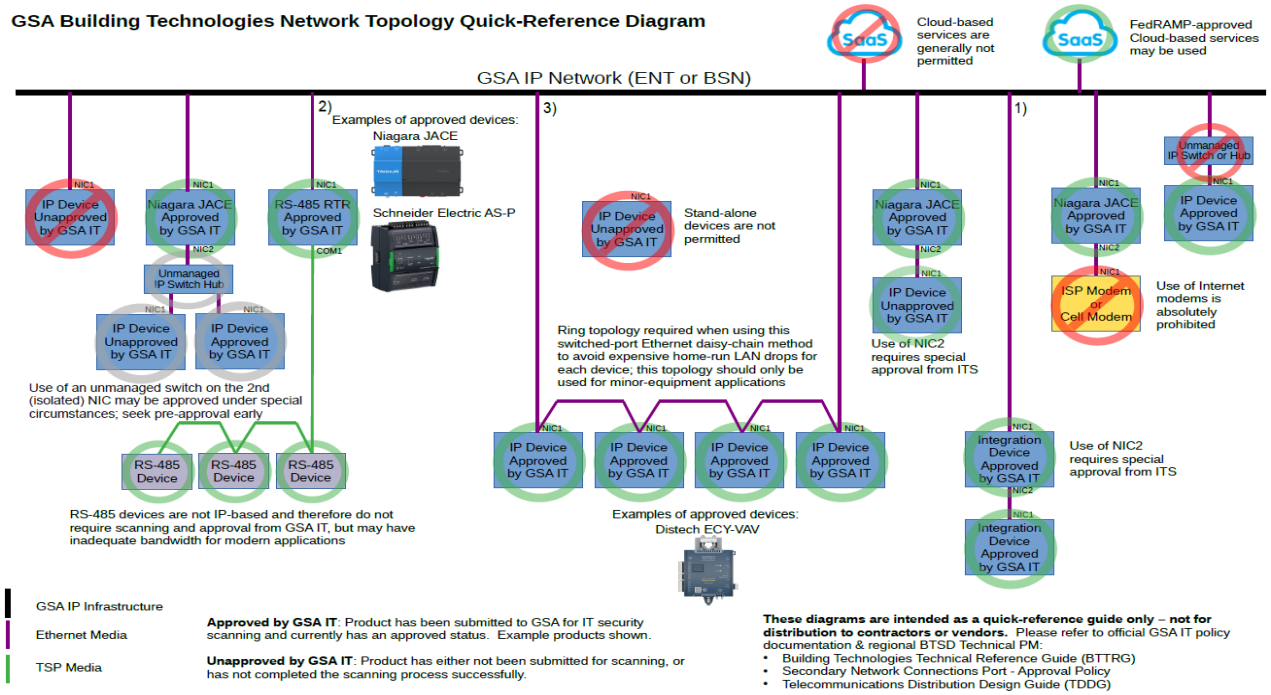


**Figure 3-1: Approved Network Topology**

### 3.1.4 BMC Assessment Identification Form

Once the BMC Assessment Team has approved the presented configuration of the device for assessment, a Device Assessment Identification form is provided to the vendor via email (See Appendix A for a link providing access to this form). This document provides the vendor information with the static IP address to configure the device for the BMC Assessment Lab environment. This document also requests the vendor provide the shipment tracking number to the BMC Assessment Team and verify the appropriate power supply is shipped with the device. The Assessment Identification Form also serves as verification from the vendor acknowledging that all requested steps for submission have been completed, and that any incomplete submission will result in a delay or rejection of the assessment.

This document should be included by the vendor in the shipment of the device when sent to the BMC Assessment Lab or emailed to the BMC Assessment Team prior to the start of the assessment.

Before shipping the device, the device must be configured with the following:

- The device must have sufficient access controls, including:
  - Login screen.
  - Password field on the login screen must be masked.
  - Passwords must meet GSA policy strength requirements: passwords must contain a minimum of eight (8) characters with uppercase and lowercase letters, symbols, and numbers.
  - Logins must be encrypted
  - An automatic logout must be configured when inactive for 15 minutes or more.

- A warning banner on the login screen must be displayed, and configurable.

- The device must be capable of managing user access rights:
  - Least privilege – nobody should have more rights than needed (e.g., 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 (e.g., administrators, general users)

- The device must be capable of utilizing Transport Layer Security (TLS) (Secure Sockets Layer [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 (e.g., metering data, energy use data, sensitive data)
  - Have TLS v1.2 encryption or higher with High Strength ciphers enabled only. Disable SSL v1.0, SSL v2.0, SSL v3.0, TLS v1.0, and TLS v1.1 ***Please Note: TLS v1.3 will become a requirement in the future. Please confirm the latest policy with the BTSD PM.***
  - All web-based logins must utilize TLS v1.2
  - Configured HTTPS to be enabled and HTTP disabled
  - Enable HTTPS Strict Transport Security (HSTS)
  - Passwords at rest must be encrypted and hashed with AES 256 bit at minimum
  - Be configured with FIPS 140-2 Compliance (Level 1 at minimum)

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

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

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

***Please Note: Any configuration required by IT Security or lack of documentation may result in delaying the security evaluation process. Contact BMC.IT.Security@gsa.gov for any further questions regarding this process. Once IT Security is ready to receive the device, they will provide detailed instructions about shipment.***

### 3.1.5 SCS Server Availability

SCS is tested in a GSA managed server environment. The BMC Assessment Team has limited servers available at any given time. Each BMC Solution SCS installed is maintained on the server throughout the remediation process. The current operating system supported for software assessments is Windows Server 2022. Linux images are available but limited only to Linux distributions for which GSA has a hardening guideline established. Creation of a Linux image is performed by GSA TechOps, with a Service Level Agreement (SLA) of ten (10) business days to provide a server image. Once a request for SCS assessment is submitted, it is added to the BMC Assessment Lab queue. BMC Stakeholders determine prioritization of software assessments.

### 3.1.6 BMC Assessment Prioritization Process

Once the device is received in the BMC Assessment Lab, it must be prioritized and placed in the lab queue. The BTS Division hosts a bi-weekly device prioritization meeting with the Office of Facility Management Leadership. This meeting is used to determine the testing order of device assessments submitted to the lab and identify the higher priority projects across PBS.

**Note:** The priority of each assessment is determined by the BMC Stakeholders and not the BMC Assessment Team or the BTS Division. Any change in priority is determined through this process and is approved by the BMC Stakeholders.

### 3.1.7 BMC Risk Categorization

GSA IT Security, in conjunction with the BTS Division, has established a risk management framework-style categorization Based on BMC functionality, capability, and network deployment. Each BMC solution submitted for an assessment is categorized based on established risk criteria. The risk categorization identifies the risk level the BMC solution can introduce into the GSA network environment. The established risk levels are low, moderate, and high. The risk categorization correlates to the level of assessment required by the BMC Assessment Team. However, if the BMC Assessor identifies a potential vulnerability during the initial assessment procedures, additional assessment measures and potential risk elevation may occur. The Risk Determination process is calculated by the information provided on the ARF. The categorization process is internal to the BMC Assessment Team. Access to this process is not granted to anyone outside of the BMC Assessment Team.

## 3.2 Step 2: BMC Assessment Lab Induction

Once the pre-assessment phase is complete, the device moves into the BMC Assessment Lab Induction phase. During this phase, attempts are made to ensure all tools necessary for the assessment are present and operational. Table 3-2 summarizes the responsibilities, expectations, and tracking of Step 2, BMC Assessment Lab Induction.

**Table 3-2: BMC Assessment Lab Induction**

| Step 2 | Responsibilities, Expectations, and Tracking for BMC Lab Induction |
|---|---|
| Responsible Role(s) | BMC Assessment Team, Vendor (when troubleshooting is required) |
| Internal Tracking Requirement | 1. Update BMC Smartsheet page indicating that the solution has been accepted OR rejected.<br>2. BMC Assessment Team verifies power on the device and tests network connectivity.<br>3. For SCS, the BMC Assessment Team validates server availability, verifies software pre-installation requirements are met, and coordinates an installation meeting with the BMC vendor. |
| Expected Response Time | ≤ 2 business days |

### 3.2.1 BMC Device 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 BMC Vendor during this process. If, after ten (10) business days, the assessor is unable to access the device or establish network connectivity, the priority is moved to the bottom of the queue until the issues are corrected. If the device is not corrected within 20 business days, it is 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 is

updated to identify the configuration deficiency and the assessment is closed. At this point, the device is shipped back to the vendor within 5 business days. The vendor is notified and provided the shipping tracking number.

### 3.2.2 SCS Induction

An SCS is considered inducted when a server has been reserved, or image build completed by GSA TechOps, all installation files are available, and 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 should be provided to the BMC Assessor prior to the installation meeting.

The following considerations prevent SCS induction from having an established SLA:

- Limited server availability;
- BMC Vendor availability;
- Installation or licensing errors; and
- SCS assessed in conjunction with a BMC device.

## 3.3 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 to test all aspects of a solution. The sections below provide additional detail on each assessment step. Appendix A provides a link where a more detailed breakout of the SLA timetable for each component described below is available. The SLA response time starts once 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 is updated to reflect the status of each assessment item noted below. Table 3-3 summarizes the responsibilities, expectations, and tracking of Step 3, BMC Assessment.

**Table 3-3: BMC Assessment**

| Step 3 | Responsibilities, Expectations, and Tracking for BMC Assessment |
|---|---|
| Responsible Role(s) | BMC Assessment Team |
| Internal Tracking Requirement | 1. Update BMC Smartsheet page to indicate the date the assessment began.<br>2. Automated scanning (Nessus, Nmap, Invicti (formally Netsparker), manual assessment checklist, and wireless testing (if applicable).<br>3. Documentation review is also conducted during this step. If any missing documents are identified, it is marked as a finding. |
| Expected Response Time (all device assessment steps) | ≤ 17 business days |

### 3.3.1 BMC Device Automated Assessment Tools and Scanning

The BMC Device Assessment process includes testing using automated scan tools. These tools are used to identify any known vulnerabilities at the device's operating system, web layer, and network layer of the device. Not all scans are necessary for each assessment. The scan requirement for each assessment is determined based on the functionality of the device and is documented in the Security Assessment Report (SAR). If possible, the BMC Assessor will conduct an authenticated scan on the BMC device. If the authentication is not supported, an unauthenticated scan will be completed.

The following scan tools are available during the BMC Device Automated Assessment Testing:

- Nessus - This tool is used to identify any known vulnerabilities at the operating system level and network layer.
- Invicti - This tool is used to identify any known vulnerabilities at the web layer of the device. If the device does not have a web application, this scan is not required.
- Nmap - This tool is used to identify what hosts, services and/or ports are available at the network level.

Once the scanning is complete, a vulnerability report is generated to identify any vulnerabilities or weaknesses. The report also provides the severity of risk each vulnerability presents, typically documented as informational, low, moderate (or medium), high, or critical. Table 3-4 provides a comparison between the Common Vulnerability Scoring System (CVSS) Base Score provided in the scan tool to CVSS risk severity. Both CVSS v2.0 and CVSS v3.0 ratings are displayed as different tools currently using different versions of the CVSS ratings.

**Table 3-4: CVSS Base Score to Severity**

| CVSS v2.0 Base Score | CVSS v3.0 Base Score | Severity |
|---|---|---|
| | 9.0 – 10.0 | Critical |
| 7.0 – 10.0 | 7.0 – 8.9 | High |
| 4.0 – 6.9 | 6.9 – 4.0 | Medium |
| 0.0 – 3.9 | 0.1 – 3.9 | Low |
| | 0.0 | None |

### 3.3.2 BMC Device Manual Assessment

The manual assessment of a BMC Device involves a deeper review of the documentation identified in Section 3.1.2, supporting software, and exploring any administrative interfaces to the device, whether via management software, through a web interface, or other means. Key areas tested in the manual assessment include:

- Vendor documentation
  - Installation instructions
  - Account management
  - Logging and monitoring
  - Device configuration and hardening requirements
  - Patch management
  - Ports and services requirements and justification

- Device Review
  - Communication methods
  - Encryption protocols and requirements
  - Firmware, Operating System, and software hardening requirements

The BMC Assessor completes the manual assessment checklist against NIST SP 800-53/NIST SP 800-213A controls (see Appendix A) to document the results of each test case. The checklist provides supporting justification for acceptable solutions as well as identifies any deficiencies in test results. Each deficiency noted in the test cases has a corresponding risk level and is documented in the SAR as an open issue.

### 3.3.3 SCS Assessment

Any SCS introduced into the GSA IT environment must be approved through the GSA Technical Standards Committee (TSC). This review has several components including security assessment of the software, 508 compliance, legal review, and a vote by the Standards Committee members. Once the software has been approved, it is posted on GSA Enterprise Architecture (EA) Analytics & Reporting (GEAR) website. Security assessments for server software are completed in the BMC Lab. Desktop software however, is reviewed by another security group within GSA-IT. For more information about submitting desktop software for review, visit the GSA IT Standards page on Insite.

#### 3.3.3.1 SCS Automated Assessment Tools and Scanning

The SCS assessment process includes testing using automated scan tools. These tools are used to identify any operating system vulnerabilities introduced by the SCS installation, web layer, software programming, and communication between the software and BMC device, if submitted in conjunction with the SCS. Pre- and post-installation scans are conducted as a part of the standard baseline process to identify BMC device-specific vulnerabilities.

The following scan tools are available during the SCS Automated Assessment Testing:

- Tenable Nessus - This tool is used to identify any known vulnerabilities at the operating system level and network layer.
- Invicti - This tool is used to identify any known vulnerabilities at the web layer of the device. If the device does not have a web application, this scan is not required.
- Nmap - This tool is used to identify what hosts, services and/or ports are available at the network level.

Once the scanning is complete, a vulnerability report is generated to identify any vulnerabilities or weaknesses. The report establishes severity in an identical manner as described in Section 3.3.1 and Table 3.2.

#### 3.3.3.2 SCS Manual Assessment

The manual assessment of a BMC Solution SCS involves a deeper review of the documentation identified in Section 3.1.2, supporting software, and exploring any administrative interfaces to the SCS, whether via management software, through a web interface, or other means.

Key areas tested in the manual assessment include:

- Vendor documentation

  - Installation Instructions
  - Account management
  - Logging and monitoring
  - Patch management
  - Ports and services requirements and justification
  - End-User License Agreement
- SCS Review
  - Communication methods
  - Encryption protocols and requirements
  - Software hardening and requirements
  - Secure programming
  - Secure Plugin Activation
  - Software Access Control
  - NIST NVD Vulnerabilities

### 3.3.4 Wireless Assessment

If a BMC solution requires wireless functionality in the GSA environment, a separate wireless assessment must be completed. Network diagrams, commissioning instructions, and protocol specifications are required documents for submitting a Wireless Assessment Request. Wireless solutions should be submitted to the BMC Assessment Lab without being commissioned. Any solution submitted post-commission is decommissioned and then recommissioned by the BMC assessor. This is due to the fact that many solutions are commissioned onsite, and the level of risk presented during commissioning needs to be assessed. Assessment procedures vary depending on the wireless protocol submitted. Proprietary solutions may take longer to assess due to the unavailability of an established attack framework or a potential acquisition of testing equipment. SLAs for wireless assessments cannot be defined due to the following factors: protocol submitted, solution architecture, and test equipment availability.

Wireless technologies must have a minimum level of AES 256-bit encryption, with the only exception being Zigbee, which currently does not support AES 256-bit encryption. All 802.11 solutions must adhere to CIO 2100.2C: “GSA Wireless Local Area Network (WLAN) Security," before being connected to the GSA network. Additionally, other non 802.11 wireless solutions are required to be scanned, remediated, and the solutions evaluated and approved by GSA-IT Security in advance of any implementation. The use of compromised or weak wireless technology results in broken encryption that can be exploited to leak sensitive information and is not permitted. These include:

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

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

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

- ZigBee Requirements
    - AES-128 bit level encryption is implemented
    - Each new pairing requires a unique handshake
    - The 802.15.4 Medium Access Control (MAC) Layer is encrypted
    - The ZigBee Network Layer is encrypted
    - The ZigBee Application Layer is encrypted
    - The vendor has not implemented any publicly known encryption keys
    - The master key is not transferred over Cleartext before encryption
    - ZigBee is 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 is 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 (e.g., "Security Mode 1" does not enable encryption, and therefore should never be used).

For additional details on the testing process and requirements for wireless devices, please refer to Appendix A for a link providing access to the “RF/Wireless Frameworks.”

### 3.3.5 Multi-Component BMC Solution

For any BMC solution that has multiple components e.g., wired, wireless, software), a SAR is issued for each individual component. Depending on the complexity of the solution and number of components submitted for assessment, the SLAs detailed may not be met.

### 3.3.6 Remote Assessment

On occasion, a BMC device cannot be shipped to the BMC Assessment Lab due to size, weight, or other constraints. If the main components cannot be separated from their housing unit and submitted, then an alternative remote assessment must be completed. This type of assessment should only be utilized when there is a significant business reason for not sending a device to the lab.

A remote assessment request is reviewed on a case-by-case basis and an assessment approach is determined at the time of submission. A previously completed remote assessment will not be used as a precedent for future remote assessments on new devices. In the event

travel is required to assess a device, appropriate funding must be provided by the customer to support this review.

#### 3.3.6.1 Rules of Engagement (RoE)

If a remote assessment justification is accepted by GSA IT, an RoE is required to approve the scanning of the device, web application, cloud solution, and/or any IP addressable connection in the proposed solution. The RoE identifies the roles, tools, system owners, methods, and boundaries of assessment. The RoE must be signed by the vendor, BMC Stakeholders, and the BMC Assessment Team prior to the start of a remote assessment.

### 3.4 Step 4: BMC Solution SAR Issuance

Upon completion of the BMC Solution Security Assessment, the BMC Assessment Team documents all findings and vulnerabilities in a SAR (See Appendix A for a link providing access to the SAR Template). Table 3-5 summarizes the responsibilities, expectations, and tracking of Step 4, BMC Solution SAR Issuance.

**Table 3-5: BMC Solution SAR Issuance**

| Step 4 | Responsibilities, Expectations, and Tracking for BMC Solution SAR Issuance |
|---|---|
| Responsible Role(s) | BMC Assessment Team |
| Internal Tracking Requirement | 1. The BMC Assessment Team creates the SAR document and updates the finding count on the BMC Smartsheet page.<br>2. The BSN ISSM reviews the SAR for QA and marks comments for the Lead Assessor to review.<br>3. Once the SAR is finalized, update the BMC Smartsheet page to indicate the date the assessment report was issued.<br>4. Distribute the SAR to the vendor, PM, and BTS Division stakeholders.<br>5. A review meeting is held with the vendor to go over the SAR.<br>6. If applicable, update the BMC Smartsheet page to indicate that the device has been remediated. |
| Expected Response Time | ≤ 3 business days |

The SAR provides a discussion of the security assessments results in Section 3 which details the finding number, finding name, description, associated NIST SP 800-53/800-213A controls or IoT Act compensating controls, any GSA policy reference, and a recommended fix. This section of the SAR is utilized within the remediation phase detailed in the following section to provide vulnerability tracking and comment responses pertaining to the remediation effort. The SAR also includes the scan reports and the manual assessment checklist completed during the assessment process.

The final BMC Solution SAR is disseminated via email and Google Drive by the BMC Assessment Team for distribution to the BMC Stakeholders and BMC Solution Vendor. All critical, high, or moderate severity findings must be resolved before the BMC component can be considered remediated. It is also important to note that reports sent outside of the GSA network (non-GSA email addresses) MUST be zipped via WinZip and encrypted with a password prior to

transmission. The password to the encrypted message must be sent via a separate email or channel (e.g., email, text, telephone). Passwords must be unique for each device vendor/manufacturer. If a BMC vendor email server does not accept zipped files, a GSA Affiliated Customer Account (GACA) may be acceptable for documentation transfer.

The BMC Assessment Team updates the associated BMC Smartsheet page with the SAR creation and issuance date.

## 3.5 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 findings. The SAR remediation phase begins once the SAR is distributed to the BMC vendor and appropriate BMC stakeholders and is a separate process from the BMC Device Assessment Phase. The remediation phase is an essential step for providing mitigating evidence and working towards the correction of open vulnerabilities of the BMC solution. This process is highly dependent on full participation from the BMC vendor, BMC Assessment Team, and BMC stakeholders. Table 3-6 summarizes the responsibilities, expectations, and tracking of Step 5, BMC vendor remediation.

**Table 3-6: BMC Vendor Remediation**

| Step 5 | Responsibilities, Expectations, and Tracking for BMC Vendor Remediation |
|---|---|
| Responsible Role(s): | BMC Assessment Team and device vendor/manufacturer |
| Internal Tracking Requirement: | 1. Device vendor provides mitigation to open items, and BMC Assessment Team validates. A re-scan is required to confirm closure.<br>2. BMC Assessment Team to archive data, notify BMC vendor, and update the BMC Smartsheet page to reflect the remediation status. |
| Expected Response Time: | ≤ 120 business days |

The subsections below provide additional details on the process and procedures included in Step 5.

### 3.5.1 Device Remediation Process Meeting

Once the BMC Assessment Team distributes the final BMC solution SAR to the BMC vendor and appropriate BMC stakeholders, a BMC remediation process meeting is scheduled. This meeting is used to communicate the process and requirements for a device to be classified as remediated.

The following agenda items are discussed during the meeting:

- Explanation of the SAR document, its purpose, and how to interpret the sections within the document.
- High-level review of each finding noted in the SAR.
- High-level review of how to mitigate each finding and acceptable remediation plans/steps.

- How communications and supporting evidence should be provided to the BMC Assessment Team.
- How to document remediation plans and milestone dates within the SAR document.
- Discuss any other questions, comments, concerns for the BMC solution.

### 3.5.2 Remediating Open Findings

Most BMC solutions will have several critical, high, or moderate severity findings which must be addressed by the BMC vendor before the solution can be categorized as remediated. The GSA understands that the BMC vendor requires time to research each finding and test an acceptable solution. The BMC Assessment Team is available throughout the remediation process to answer any questions or provide guidance for outstanding issues.

The device/software manufacturer POC is expected to provide supporting evidence and justification for each open finding before it can be accepted and closed. The BMC Assessment Team cannot close any findings without acceptable supporting information. All remediation progress is tracked in Section 3 of the SAR. The BMC vendor and the BMC Assessment Team uses the following process to track each open finding:

The device/application manufacturer POC is responsible for:

- Documenting the remediation plan in the “Remediation Plan” section of each finding. This should provide enough details for the BMC Device Assessment Team to understand how each corrective action plan will be implemented. This section can be updated throughout the process if additional information is needed during the remediation phase.
- Identifying a remediation date in the “Scheduled Completion Date” field. This date is used to identify the date the BMC Vendor will provide a remediation plan to support the closure of the vulnerability.
- Providing supporting documentation by either embedding files into the SAR document or emailing additional documents to support each action plan.
- Providing firmware updates for devices or software updates for SCS solutions.

The BMC Assessment Team is responsible for:

- Reviewing each mitigation plan provided in the “Remediation Plan” section of each vulnerability table.
- Performing a remediation scan after a firmware update for a BMC device or a software update for an SCS is applied to close out these findings.
- Documenting a response to the vendors/manufacturer’s remediation plan in the “GSA IT Security Comments” section of each finding. The BMC Assessment Team will document the date of the comment, initials of the assessor and identify if the remediation plan is accepted or incomplete. This section also identifies any additional questions or comments for the vendor/manufacturer.
- Documenting the remediation status and completion date in the “Finding Control #” header and the “Actual Completion Date” field. Both of these items will only be updated when a remediation plan is accepted, and the vulnerability is considered closed.
- Reviewing the SAR and providing a response to the vendors/manufacturer POC within ten (10) business days of receiving any updates to the report.

The official SAR version is stored on the internal GSA BMC Google Drive as updates are made throughout the remediation process. The BMC Assessment Team is responsible for distributing the latest version of the SAR to all parties. The BMC Assessment Team will also track remediation progress through the BMC Smartsheet page assigned to the device.

### 3.5.3 Remediation Decision

If the BMC Assessment Team can confirm that all critical, high, and moderate severity findings have been resolved, the BMC device/SCS shall be considered remediated, and the associated BMC Smartsheet page shall be identified as closed. The BMC Assessment Team is responsible for communicating all remediation decisions to the BMC vendor and BMC stakeholders. The applicable BMC solution is added to the remediated BMC solution list on GSA's BTS Division Smartsheet page.

Note**:** The Smartsheet page is restricted to BMC IT Security and PBS personnel. Access can be requested from BMC IT Security.

Note: 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 are notified of the non-remediation decision and the BMC device is added to the non-remediated BMC device list on GSA's BTS Division Smartsheet page.

The BMC Assessment Team will update the Smartsheet page with the remediation status and close and archive it for historical purposes.

## 3.6 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 should not purchase any additional components of that type and model since it provides an identified risk to the GSA environment.

The BMC Assessment Team reviews 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. In the event 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 reassessment must be completed. Table 3-7 summarizes the responsibilities, expectations, and tracking of Step 6, BMC Solution Post Assessment.

**Table 3-7: BMC Solution Post Assessment**

| Step 6 | Responsibilities, Expectations, and Tracking for BMC Solution Post Assessment |
|---|---|
| Responsible Role(s) | BMC Assessment Team, BTS Division, and vendor/manufacturer |
| Internal Tracking Requirement | 1. If remediated product is resubmitted to the lab, time has elapsed since previous assessment, and major changes have been implemented, the product needs to be rescanned.<br>2. Otherwise, if minor changes are made, a comparison approval is performed and the latest version is used. |
| Expected Response Time | N/A |

### 3.6.1 Remediated Device Reassessment

If a remediated device is resubmitted to the BMC Assessment Lab, the following are used as guidelines on how to assess:

- If the SAR is less than 3 years old and the device is being submitted for review of a minor update/change in software or other configurations, no review of the device is needed.
  - Minor changes include but are not limited to: (1) an update in firmware and/or software version number that is within 10 minor release versions (e.g., 1.X or 1.1.X) of the reviewed software; (2) routine vulnerability patching and bug fixes; and (3) minor changes to the look and feel of the web application (does not change functionality).
- If the SAR is less than 3 years old and the device is being submitted for review of a major update/change in software or other configuration, new scan reports (OS, Invicti, Nmap, etc.) must be completed. Any critical, high, or moderate findings must be corrected before approval is granted.
  - Major changes include but are not limited to: (1) major update to the existing operating system; (2) major update to the installed firmware (e.g., X.0); (3) major technology changes or inclusions (enabling wireless capability or changing technical protocol); (4) a minor update in excess of 10 versions of the initially reviewed firmware; (5) addition of significant new functionality; and (6) change in web application or management software.
- If the SAR is less than 3 years old and the device is being submitted for review of a major update/ change in software and hardware, a new assessment must be performed as this is considered a new device (includes manual assessment, scans, and new SAR). Any critical, high, or moderate findings must be corrected before approval is granted.
  - Major changes include but are not limited to: (1) change in the operating system (e.g., Windows to Linux); (2) change in hardware along with a change in firmware; and (3) end-of-life transition to newer models.
- If a BMC stakeholder wishes to implement a remediated device with a SAR completed 3 or more years ago, it must be submitted for review for Step 1 of this process. Once the BMC Assessment Team reviews the latest documentation and specifications, an assessment determination is made. This is determined on a case-by-case basis and based on various criteria including but not limited to:
  - Changes in functionality since the last assessment
  - New known risks and vulnerabilities
  - New or additional identified risks to the BSN or GSA environment
  - Planned onboarding of the device into the BSN FISMA system boundary

- Implementation of routine scanning of the device in the GSA environment

**Note**: The GSA BMC Assessment Team is responsible for determining what constitutes a major or minor change.

### 3.6.2 Non-Remediated Devices Reassessment

If a device is determined to be non-remediated, no additional assessment activities or review of the current security package or BMC device SAR is performed regardless of age or updates. In the event of new or additional remediation steps for the current open BMC Device SAR findings, the vendor/manufacturer must restart the assessment process from the beginning and the device is treated as a new assessment.

## 3.7 GSA IoT Waivers

Upon identification of a need to receive a GSA IoT Waiver for a BSN solution or BMC device the OCISO will follow the IoT Waiver creation and approval process.

## Appendix A: BMC Device Templates and Forms

The IT Security Device Assessments and Submission page provides documents and links to locations where the following forms and templates mentioned in this document may be found.

- ARF Form - Google Doc
- ARF Checklist - Excel Spreadsheet
- Shipping Information

**Note:** The Google Folder at the link below is restricted to personnel involved in the BMC component assessment process. If you need access, please request it using the native Google capabilities.

The BMC Templates - SOP Appendices Google Folder includes the following documents:

- Risk Based Manual Device Checklists
- Device Assessment Identification Form Template
- BMC Device Review Timelines (Initial Review)
- RF/Wireless Framework Testing Reference
- SAR Template - Explained

## Appendix B: Points of Contact

For any questions on the BMC process or devices, please contact:

**BMC IT Security**
bmc.it.security@gsa.gov

**PBS Building IT Operations and Support**
Pbs.pbios@gsa.gov

## Appendix C: Additional References and Resources

The following links provide additional references and information.

- Building Technology Services Division
- Building Technologies Technical Reference Guide
- GSA IT Security
- Internet of Things Cybersecurity Improvement Act of 2020 (IoT Act) (Public Law 116-207)
- NIST Computer Security Resource Center Special Publications