



**IT Security Procedural Guide:
Building Automation System (BAS)
Security Assessment Process
CIO-IT Security-16-76**

Revision 1

August 29, 2018

EXECUTIVE SUMMARY

This Security Procedural Guide is intended to establish a standard process and procedures for evaluating the information technology (IT) security of a submitted Building Automation System (BAS) component for approved initial use by the General Services Administration (GSA) Public Building Service (PBS). BAS components encompass building management control (BMC) devices and supervisory control software (SCS). This process should not be used in place of the approved FISMA review process for the Building Services Network (BSN) at GSA. This document formalizes the workflow, provides associated time frames for each process step, and establishes the criteria used to identify the risk posture presented by the BAS within the PBS environment. These test procedures can be used to supplement the approved FISMA review process.

This Guide identifies six essential process steps in reviewing the risk posture of each BAS component submitted to the BMC Assessment Lab. These steps include:

- **Step 1: BAS Pre-Assessment (≤30 Business Days):** This step focuses on the collection and identification of the following information; BMC device specifications and configuration settings, and SCS server configurations and installation requirements. Documentation is provided by the BAS Vendor and reviewed by the BMC Assessment Team. If the BMC device meets all pre-assessment requirements, it will be inducted to the lab. If the SCS meets all pre-assessment requirements, the software will be inducted and an installation meeting with the BAS vendor will be coordinated.
 - **Requirements:** Electrical specifications, installation guides, user manuals, technical specifications, and the Assessment Request Form(s).
- **Step 2: BAS Assessment Lab Induction (≤ 2 Business Days):** The key tasks for this step are identified as follows; for BMC devices, the BMC Assessment Team will attempt to power on the device and establish network connectivity, For SCS, the BMC Assessment Team will validate server availability, verify software pre-installation requirements are met, and coordinate an installation meeting with the BAS vendor.
 - **Requirements:**
 - **BMC Device:** Provide the power supply identified in technical specifications and configured how it will be install in a GSA environment, if configuration varies from a device's commercial deployment.
 - **SCS:** Assign server, if available, ensure install of GSA hardened supplemental services (SQL Server, IIS, Apache, etc.), software license, and have a BAS vendor POC. Note that the BMC Assessment Team has a limited number of test servers available. Due to this constraint, SCS is not held to the identified lab induction Service Level Agreements (SLAs).
- **Step 3: BAS Assessment (≤ 17 Business Days):** The BAS 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 various tests include running automated scan tools to identify weaknesses, a manual assessment of operational and management processes, and wireless functionality testing and review (if applicable).

- **Requirements:** Automated Scanning (Nessus, Nmap, web vulnerability scanner), manual assessment checklist, and wireless testing (if applicable).
- **Step 4: BAS Security Assessment Report (SAR) Issuance (≤ 3 Business Days):** The SAR identifies vulnerabilities and weaknesses found during the BAS Assessment process. All critical, high, and moderate weaknesses documented in the SAR must be corrected before the BMC Device or SCS can be classified as remediated.
 - **Requirements:** Creation and distribution of initial SAR.
- **Step 5: BMC Device Vendor Remediation (≤ 120 Business Days):** A BAS is required to go through the remediation process if the SAR is issued with open critical, high, or moderate findings. The remediation phase is an essential step for providing mitigating evidence and working towards the correction of open vulnerabilities on the BAS component. This process is highly dependent on full participation from the BAS Vendor, BMC Assessment Team, and PBS Stakeholders. If a BAS is identified as non-remediated, GSA should not purchase any additional devices or software packages of that model or version, since it provides an identified risk to the GSA environment.
 - **Requirements:** BAS vendor provides mitigation to open items, and BMC Assessment Team validates.
- **Step 6: BAS Post Assessment (Reviewed on case-by-case basis):** In the event that the device or software undergoes changes as a part of a System Development Life Cycle (SDLC) process, there may be a need to reassess the BAS. Additionally, in the event of any security issue or incident, BAS components may be required to be re-assessed or reviewed.
 - **Requirements:** Assessment determination based on remediation status, new known risks, or new functionality enabled.

It is important to note that participation and timely responses from BAS Vendors, the BMC Assessment Team, the Building and Energy (B&E) Team, and other PBS Stakeholders is essential for a successful BAS assessment. Each step in this process identifies SLAs that stipulate the acceptable amount of time for actions and deliverables. Failure to meet these SLAs could delay progress and acceptance of a BAS remediation decision.

Lastly, this process guide is meant to document the current practices used in the BMC Assessment Lab. GSA IT realizes that as the BAS industry matures and more stringent hardening and security requirements are implemented, this process will need to adapt to the changing environment. This guide will be updated to reflect any change in processes and will be reviewed, as necessary.

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Initial Version – 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

Approval

IT Security Procedural Guide: Building Automation System (BAS) Security Assessment Process, CIO-IT Security-16-76, Revision 1 is hereby approved for distribution.

8/30/2018

10/1/2018

X Bo Berlas

Bo Berlas
Acting GSA Chief Information Security Officer
Signed by: General Services Administration

X Philip Klokis

Philip Klokis
Associate Chief Information Officer (IP)
Signed by: General Services Administration

Table of Contents

1	Introduction	3
1.1	Purpose.....	3
1.2	Policy and Guides.....	3
2	BAS Security Assessment Process.....	4
2.1	Step 1: BAS Pre-assessment	4
2.1.1	BAS Security Assessment Request Form.....	5
2.1.2	BAS Documentation Verification and Review.....	6
2.1.3	BAS Technical Prerequisites and Review	6
2.1.4	BAS Assessment Identification Form	8
2.1.5	SCS Server Availability.....	8
2.1.6	BAS Assessment Prioritization Process.....	8
2.1.7	BAS Risk Categorization	8
2.2	Step 2: BAS Assessment Lab Induction.....	9
2.2.1	BMC Device Induction.....	9
2.2.2	SCS Induction	9
2.3	Step 3: BAS Assessment.....	10
2.3.1	BMC Device Automated Assessment Tools and Scanning.....	10
2.3.2	BMC Device Manual Assessment.....	11
2.3.3	SCS Assessment.....	12
2.3.4	Wireless Assessment	13
2.3.5	Multi-Component BAS Solution.....	13
2.3.6	Remote Assessment.....	13
2.4	Step 4: BAS Solution SAR Issuance	14
2.5	Step 5: BAS Vendor Remediation	15
2.5.1	Device Remediation Process Meeting	15
2.5.2	Remediating Open Findings.....	16
2.5.3	Remediation Decision	17
2.6	Step 6: BAS Solution Post Assessment	17
2.6.1	Remediated Device Reassessment	18
2.6.2	Non-Remediated Devices Reassessment.....	19
	Appendix A: BMC Device Templates and Forms	20
	Appendix B: Points of Contact.....	21
	Appendix C: Additional References and Resources	22
	Table 2.1-1: BAS Pre-assessment	5
	Table 2.2-1: BAS Assessment Lab Induction.....	9
	Table 2.3-1: BAS Assessment	10
	Table 2.3-2: CVSS Base Score to Severity	11
	Table 2.4-1: BAS Solution SAR Issuance	14
	Table 2.5-1: BAS Vendor Remediation.....	15
	Table 2.6-1: BAS Solution Post Assessment	18

1 Introduction

The GSA PBS owns or operates over 1,500 buildings on behalf of Federal, State, and Local agencies. The ability to automate and centrally control building management functions such as heating, ventilation, and air conditioning (HVAC), lighting, and logical and physical access control, is an increasingly desired capability in order to support carbon footprint reduction and “Go Green” initiatives.

BAS solutions are a subset of Industrial Control Systems (ICS) (also referred to as Operational Technology (OT)), which support this automation and centralized control, through the ability to logically and physically connect BAS components to traditional IT networks. BMC devices can be managed via a SCS, or can operate independently.

As the ICS field is a maturing discipline, the GSA recognizes that not all BAS solutions meet the requirements typically incorporated into mainstream IT hardware and software products. However, in order to achieve the GSA’s mission, and to meet the GSA’s 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 BAS solutions proposed for use within GSA owned facilities.

1.1 Purpose

The purpose of this guide is to define the procedures for assessing BAS solutions submitted to the GSA OCISO by the PBS-IT Building and Energy (B&E) Team. This process is designed to ensure that a reasonable level of due diligence is taken, through an initial security evaluation of each BAS solution’s technical, operational, and management capabilities, such that the BAS solution’s vulnerabilities are identified and remediated prior to their installation into GSA IT network environments. This document also formalizes the workflow and associated time frames for each step in the process.

1.2 Policy and Guides

GSA IT Security Policy, CIO 2100.1, states:

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 PBS-IT: Building Technologies Technical Reference Guide, dated September 29, 2016, states:

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 PBS stakeholders and the vendor. The assessment report will allow GSA to understand and accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. The contractor/vendor 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.

2 BAS Security Assessment Process

The following sections describe the major steps and significant sub-components involved in the BAS Security Assessment Process. Each step includes a table indicating the 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 will increase the delivery and/or response time for each step.

Please note that an assessment will only be conducted for BAS solutions already procured by GSA. There will be no pre-scanning of BAS solutions prior to contract award. Furthermore, each BAS component submitted to the lab must have an assigned project sponsor who must provide information on the current project plan to implement the device.

Trello is used to track the project development and workflow for all BAS solution assessment projects. Access to the BMC Trello Boards will be limited to the BMC Assessment team. A status update on BAS solution assessments will be provided to the B&E team on a weekly basis and will be communicated to other stakeholders as needed.

2.1 Step 1: BAS Pre-assessment

The B&E Team is responsible for working with BAS Vendors to identify BAS solutions needing assessment. During this stage, the B&E Team will collaborate with the BAS 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 BAS solution into the BMC Assessment Lab. Table 2.1-1 summarizes the responsibilities, expectations, and tracking of Step 1, BAS Pre-assessment.

Table 2.1-1: BAS Pre-assessment

Step 1	Responsibilities, Expectations, and Tracking for BAS Pre-assessment
Responsible Role(s):	PBS-IT B&E Team, GSA BMC Stakeholders, BAS Vendor, BMC Assessment Team
Internal Tracking Requirement:	<ol style="list-style-type: none"> 1. Review BMC ARF and corresponding information 2. Validate technical specifications and requirements 3. Create Trello card if all pre-assessment requirements are met and determine risk level 4. Distribute BMC Assessment Identification Form 5. Identify and update device prioritization
Expected Response Time:	≤ 30 business days Note: BMC Assessment Lab acceptance response time is dependent upon the timeliness and quality of vendor documentation delivery, the B&E Team response time and BMC Stakeholder prioritization process.

2.1.1 BAS Security Assessment Request Form

The BMC Security Assessment Request Form (ARF) is the first requirement in the pre-assessment phase and must be submitted prior to shipping the device or installing the software to the BMC Assessment Lab. This form provides 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 Assessment Request Form (ARF) (*Required*)
 - A link providing access to the BMC ARF can be found in [Appendix A](#).
 - The BMC ARF must be completed by the BAS Sponsor and/or B&E Project Manager before the device is shipped to, or software is installed in, the BMC Assessment Lab.
 - All required fields, identified with an “*”, must be completed in order to submit the final form.
 - Prior to submitting the form, upload all files associated with software or device to the link provided in the ARF.
 - It is important to note, responses that provide more complete information and details, will lead to a more thorough and timely assessment.
- Device Checklist Spreadsheet (*Optional - For use by PMs to collect vendor information*)
 - The Checklist Spreadsheet is meant for provision to the vendor by the PM for information collection. The Device Checklist Spreadsheet enables data gathering from vendors who cannot access the GSA Google Tools and Drives. The Device Checklist Spreadsheet is identical to the BMC ARF, making data input into the BMC ARF for the PM's easier.
 - The Device Checklist Spreadsheet is optional, as its use is at the discretion of the PM to help facilitate and coordinate the collection of required information.

- Any sensitive information being collected in this process should be handled with care and appropriate security steps used, such as GSA-approved file encryption.
- A link to the latest version of the Device Checklist Spreadsheet can be found in [Appendix A](#).

2.1.2 BAS Documentation Verification and Review

All BMC Device and SCS requests must be accompanied by system documentation commensurate to 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 BAS 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; FCC ID, protocol specification, operational documentation, commissioning guides, and any standards accreditation documents, i.e., Zigbee Alliance accreditation.
3. Operation & Maintenance Guide(s) for all the hardware, firmware, and software submitted for assessment. Note that this must include the BAS Vendor's life cycle support schedule and service agreement for hardware, firmware, and software updates due to identified security vulnerabilities.
4. User's 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 any missing items or gaps in documentation, a notification will be sent to the BAS Vendor, B&E PM, and GSA 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 Trello Board will be updated to reflect the lack of information and the assessment identified as closed.

2.1.3 BAS Technical Prerequisites and Review

The BMC Device should 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 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 will either be returned for proper configuration or the BMC Device assessment will be placed on hold until the BAS 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 Trello Board will be updated to reflect the configuration deficiency and the assessment will be marked as closed.

The BMC Device should 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 will be immediately rejected without further review. The BMC Trello Board will be updated to identify the technical deficiency and the assessment will be closed.

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

- No Remote Access (back doors) from outside of the GSA network – access must use GSA provided access (Citrix, VDI, or GFE with VPN).
- Use of third party providers (cloud, hosting, etc.) are restricted to only GSA approved and FISMA reviewed third party providers.
- Protocols such as Telnet, TFTP and FTP, HTTP, will not be accepted due to the unencrypted nature of the protocols per NIST SP 800-53, Revision 4, CM-7 Least Functionality:
 - “Organizations review functions and services provided by information systems or individual components of information systems, to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, and file sharing). Organizations consider disabling unused or unnecessary physical and logical ports/protocols (e.g., Universal Serial Bus, File Transfer Protocol, and Hyper Text Transfer Protocol) on information systems to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling.”
- Device should not allow changes to security configuration without authentication.
- Device should 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), 802.11 WEP/WPA and low level frequency without protection, such as GSM Band and CDMA (3G/4G/LTE).
- BACnet will be reviewed on a case by case basis.
 - BACnet/Ethernet- Because Layer 2 network traffic cannot be effectively managed on the GSA network between subnets, BACnet/Ethernet is expressly prohibited from being implemented on the GSA WAN. BACnet/Ethernet can be used at a given field site, provided all BACnet devices are on the same subnet.

- BACnet/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.

2.1.4 BAS Assessment Identification Form

Once the BMC Assessment Team has approved the presented configuration of the device for assessment, a Device Assessment Identification form will be provided to the vendor via email (See [Appendix A](#) for a link providing access to this form). This document will provide 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.

2.1.5 SCS Server Availability

SCS is tested in a GSA managed server environment. The BMC Assessment Team has a limited number of servers available at any given time. Each BAS Solution SCS installed is maintained on the server throughout the remediation process. The operating system supported for software assessments is Windows 2012R2. 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 an SLA of 10 business days to provide a server image. Once a request for SCS assessment has been submitted, it will be added to the BMC Assessment Lab queue. Prioritization of software assessments is determined by BMC Stakeholders.

2.1.6 BAS Assessment Prioritization Process

Once the device is received in the BMC Assessment Lab, it must be prioritized and placed in the lab queue. The B&E Team 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. Please note that the priority of each assessment is determined by the BMC Stakeholders and is not by the BMC Assessment Team, or the B&E Team. Any change in priority is determined through this process and is approved by the BMC Stakeholders.

2.1.7 BAS Risk Categorization

GSA IT Security, in conjunction with the B&E Team, has established a risk management framework-style categorization based on BMC functionality, capability, and network

deployment. Each BAS solution submitted for an assessment will be categorized based on established risk criteria. The risk categorization will identify the risk level the BMC 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 identified a potential vulnerability during the initial assessments 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 will not be granted to anyone outside of the BMC Assessment Team.

2.2 Step 2: BAS Assessment Lab Induction

Once the assessment pre-assessment phase is complete, the device will move into the BMC Assessment Lab Induction phase. During this phase, attempts will be made to ensure all tools necessary for the assessment are present and operational. Table 2.2-1 summarizes the responsibilities, expectations, and tracking of Step 2, BAS Assessment Lab Induction.

Table 2.2-1: BAS Assessment Lab Induction

Step 2	Responsibilities, Expectations, and Tracking for BAS Lab Induction
Responsible Role(s):	BMC Assessment Team, BAS Vendor (when trouble shooting is required)
Internal Tracking Requirement:	Update BMC Trello Board indicating that the solution has been accepted OR rejected.
Expected Response Time:	≤ 2 business days

2.2.1 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 BAS Vendor during this process. If, after 10 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 Trello Board 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 5 business days. The vendor will be notified and provided the shipping tracking number.

2.2.2 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 BAS 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,
- BAS Vendor availability,
- Installation or licensing errors, and
- SCS assessed in conjunction with a BMC device.

2.3 Step 3: BAS Assessment

The BAS 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. [Appendix A](#) provides a link where a more detailed breakout of the SLA time table for each component described below is available. 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 time table does not include the time to mitigate issues or troubleshoot problems with the BAS Vendor. The BMC Trello Board will be updated to reflect the status of each assessment item noted below. Table 2.3-1 summarizes the responsibilities, expectations, and tracking of Step 3, BAS Assessment.

Table 2.3-1: BAS Assessment

Step 3	Responsibilities, Expectations, and Tracking for BAS Assessment
Responsible Role(s):	BMC Assessment Team
Internal Tracking Requirement:	<ol style="list-style-type: none"> 1. Update BMC Trello Board to indicate the date the assessment began. 2. Update BMC Trello Board to indicate the date each testing step was completed.
Expected Response Time (all device assessment steps):	≤ 17 business days

2.3.1 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 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 will be documented in the SAR. The BMC Assessor will conduct an authenticated scan on the BMC device, if possible. 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.
- Web Application Vulnerability Scanner - 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 will be 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 2.3-2 provides a cross walk 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 use different versions of the CVSS ratings.

Table 2.3-2: 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

2.3.2 BMC Device Manual Assessment

The manual assessment of a BMC Device involves a deeper review of the documentation identified in Section 2.1.2, 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 will complete the manual assessment checklist (see Appendix A) to document the results of each test case. The checklist will provide supporting justification for acceptable solutions as well as identify any deficiencies in test results. Each deficiency noted in the test cases will have a corresponding risk level and will be documented in the SAR as an open issue.

2.3.3 SCS Assessment

Any BAS Solution SCS introduced into the GSA IT environment must be approved through the GSA Enterprise Architecture (EA) Committee. The EA review has several approval requirements and will leverage the BAS Lab assessment as the security assessment requirement. The BAS Project Manager is responsible for submitting a request through the GSA EA Committee as well as submitting a BAS assessment request using the requirements in Step 1 above.

Note: BAS Solution SCS can only be considered approved and uploaded to GEAR if it meets both GSA IT Security and EA assessment requirements.

2.3.3.1 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 BAS/BMC Device specific vulnerabilities.

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

- Nessus - This tool is used to identify any known vulnerabilities at the operating system level and network layer.
- Web Application Vulnerability Scanner - 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 will be generated to identify any vulnerabilities or weaknesses. The report establishes severity in an identical manner as described in Section 2.3.1 and Table 2.3-2 .

2.3.3.2 SCS Manual Assessment

The manual assessment of a BAS Solution SCS involves a deeper review of the documentation identified in Section 2.1.2, 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

2.3.4 Wireless Assessment

If a BAS 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 will be decommissioned and then recommissioned by the BMC Assessor. This is due to the fact 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 no established attack framework being available; 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.

For additional details on the testing process and requirements for wireless devices, please refer to [Appendix A](#) for a link providing access to the “Wireless Assessments SOP.”

2.3.5 Multi-Component BAS Solution

For any BAS Solution that has multiple components, i.e., wired, wireless, and software, a SAR will be 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.

2.3.6 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 will have to be completed. This type of

assessment should only be utilized when there is significant business reason for not sending a device to the lab.

A remote assessment request will be reviewed on a case by case basis and an assessment approach will be 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.

2.3.6.1 Rules of Engagement (RoE)

If a remote assessment justification is accepted by GSA IT, a 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 will identify the roles, tools, system owners, methods, and boundaries of assessment. The RoE must be signed by the vendor, BAS Stakeholders, and the BMC Assessment Team creating a legally binding agreement for the assessment. The remote assessment cannot take place until all represented parties involved have signed the RoE.

2.4 Step 4: BAS Solution SAR Issuance

Upon completion of the BAS Solution Security Assessment, the BMC Assessment Team will document all findings and vulnerabilities in a SAR (See [Appendix A](#) for a link providing access to the SAR Template). Table 2.4-1 summarizes the responsibilities, expectations, and tracking of Step 4, BAS Solution SAR Issuance.

Table 2.4-1: BAS Solution SAR Issuance

Step 4	Responsibilities, Expectations, and Tracking for BAS Solution SAR Issuance
Responsible Role(s):	BMC Assessment Team
Internal Tracking Requirement:	<ol style="list-style-type: none"> 1. The BMC Assessment Team will create the SAR document and update the BMC Trello Board. 2. Once the SAR is finalized, update the BMC Trello Board to indicate the date the assessment report was issued. 3. If applicable, update the BMC Trello Board 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 controls, any GSA policy reference, and a recommended fix. This section of the SAR will be utilized within the remediation phase detailed in the following section to provide vulnerability tracking and comment responses pertaining to the remediation effort. The SAR will also include the scan reports and manual assessment checklist completed during the assessment process.

The final BAS Solution SAR will be disseminated via email and Google Drive by the BMC Assessment Team for distribution to the BMC Stakeholders and BAS Solution Vendor. All critical, high, or moderate severity findings must be resolved before the BAS 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 must be sent via a separate email or channel (e.g., email, text, telephone). Passwords must be unique for each Device Vendor. If a BAS Vendor email server does not accept zipped files, a GACA account may be acceptable for documentation transfer.

The BMC Assessment Team will update the associated BMC Trello Board card with the SAR creation and issuance date.

2.5 Step 5: BAS Vendor Remediation

A BAS 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 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 BAS Solution. This process is highly dependent on full participation from the BAS Vendor, BMC Assessment Team, and BMC Stakeholders. Table 2.5-1 summarizes the responsibilities, expectations, and tracking of Step 5, BAS Vendor Remediation.

Table 2.5-1: BAS Vendor Remediation

Step 5	Responsibilities, Expectations, and Tracking for BAS Vendor Remediation
Responsible Role(s):	BMC Assessment Team, and Device Vendor
Internal Tracking Requirement:	<ol style="list-style-type: none"> 1. Update the Trello card to reflect remediation status and close ticket 2. BMC Assessment Team to archive data, notify BAS Vendor, and update Insite status page
Expected Response Time:	≤ 120 business days

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

2.5.1 Device Remediation Process Meeting

Once the BMC Assessment Team distributes the final BAS Solution SAR to the BAS Vendor and appropriate BMC Stakeholders, a BAS 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 BAS Solution.

2.5.2 Remediating Open Findings

Most BAS Solutions will have several critical, high, or moderate severity findings which must be addressed by the BAS Vendor before the solution can be categorized as remediated. The GSA understands that the BAS Vendor will require 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 BAS Vendor 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 will be tracked in Section 3 of the SAR. The BAS Vendor and the BMC Assessment Team will use the following process to track each open finding:

The BAS Vendor 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 BAS 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.

The BMC Assessment Team is responsible for:

- Reviewing each mitigation plan provided in the “Remediation Plan” section of each vulnerability table.

- Documenting a response to the Device Vendors 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 Device Vendor.
- 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.
- The BMC Assessment Team will review the SAR and provide a response to the Device Vendor within 10 business days of receiving any updates to the report.

The official SAR version will be 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 Trello Board card assigned to the device.

2.5.3 Remediation Decision

If the BMC Assessment Team can confirm that all critical, high, and moderate severity findings have been resolved, the BMC Device shall be considered remediated, and the associated BMC Trello Board card shall be identified as closed. The BMC Assessment Team is responsible for communicating all remediation decisions to the BAS Vendor and BMC Stakeholders. The applicable BAS Solution will be added to the remediated BAS Solution list on GSA’s Insite (<https://insite.gsa.gov/portal/content/655974>).

It is important to note that the BAS Solution SAR is a snap shot in time, whose results lose relevancy over time as new vulnerabilities and exploit techniques are identified. As such, if a BAS Vendor cannot respond to the GSA with actionable remediation of the identified findings within 120 business days (six months) from the issuance of the BAS SAR, the BMC Assessment team has the right to categorize the BAS Solution as non-remediated and close the Trello card. The BAS 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 Insite (<https://insite.gsa.gov/portal/content/655974>).

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

2.6 Step 6: BAS Solution Post Assessment

Once the remediation decision has been determined, the BAS Assessment project is considered closed. If a BAS 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 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 O&M support contract is in place to support any additional remediation or upgrades to the device. In the event that 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. This section provides additional guidance for requirements as to when a re-assessment must be completed. Table 2.6-1 summarizes the responsibilities, expectations, and tracking of Step 6, BAS Solution Post Assessment.

Table 2.6-1: BAS Solution Post Assessment

Step 6	Responsibilities, Expectations, and Tracking for BMC Solution Post Assessment
Responsible Role(s):	BMC Assessment Team, PBS-IT B&E Team and Device Vendor
Internal Tracking Requirement:	To be determined based on requirements needed.
Expected Response Time:	N/A

2.6.1 Remediated Device Reassessment

If a remediated device is resubmitted to the BMC Assessment Lab, the following will be 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; (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, Webinspect, 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; (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

will be 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; (3) end of life transition to newer model.
- If a BMC Stakeholder wishes to implement a remediated device with a SAR that was completed 3 or more years ago, it must be submitted for Step 1 of this process for review. Once the BMC Assessment Team reviews the latest documentation and specifications, an assessment determination will be made. This will be determined on a case-by-case basis and will be 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 risk to the BSN or GSA environment
 - Planned onboarding of the device into the BSN A&A FISMA boundary
 - Implementation of routine scanning of the device in the GSA environment

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

2.6.2 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 will be performed regardless of age or updates. In the event of new or additional remediation steps for the current open BMC Device SAR findings, the BAS Device Vendor must restart the assessment process from the beginning and the device will be treated as a new assessment.

Appendix A: BMC Device Templates and Forms

The links below provide the location where the following forms and templates mentioned throughout this document may be found.

<https://insite.gsa.gov/portal/content/655934?term=BMC%20Scan>

- Assessment Request Form Excel Checklist
- BMC Device Assessment Request Form
- Shipping Information

<https://drive.google.com/drive/folders/0B03tcPaYeSaZTmhTSzdIMFMzdlk>

Documents provided in this folder include:

- Risk Based Manual Device Checklists
- Device Assessment Identification Form Template
- BAS Device Review Timelines (Initial Review)
- Wireless Assessments SOP
- Wireless Framework Testing Reference
- SAR Template

Appendix B: Points of Contact

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

BMC IT Security

bmc.it.security@gsa.gov

Building and Energy Systems Team

pbs.pbios@gsa.gov

The most up to date list of other key regional BMC Point of Contacts can be found on GSA's Insite page:

<https://insite.gsa.gov/portal/category/539218>

Appendix C: Additional References and Resources

The following links provide additional references and information:

GSA IT Security Page	https://insite.gsa.gov/portal/category/534722
Building and Energy Systems Insite Page	https://insite.gsa.gov/portal/category/520178
NIST IT Security Special Publications	https://csrc.nist.gov/publications/sp
PBS-IT: Building Technologies Technical Reference Guide	https://insite.gsa.gov/portal/mediaId/664598/fileName/Building_Technologies_Technical_Reference_Guide_v12_092916.action