G500 v1.1 NERC-CIP5 Response

Product Bulletin

Date: Mar 3rd, 2020 **Classification:** GE Information **Publication Number:** PRBT-0429

Overview

The purpose of this document is to answer commonly asked questions pertaining to the features supported by the version 1.1 of G500 Series of Substation Gateway products. This is not a NERC-CIP document. Users of GE Grid Solutions G500 equipment may require this information for the purposes of assessment and implementation of NERC-CIP v5 processes.

Standard	Req #	Requirement	Applicable Security Measures
CIP-002-5.1 Bulk Electric System [BES] Cyber System Categorization	All	It is left up to the Responsible Entity to determine the level of granularity at which to identify a BES Cyber System within the qualifications in the definition of BES Cyber System (…)	Not Applicable (Responsible Entity Organizational function)
CIP-003-5 Security Management Controls	R1	Each Responsible Entity, for its high impact and medium impact BES Cyber Systems, shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies (…)	Not Applicable (Responsible Entity Organizational function)
	R2	Each Responsible Entity for its assets identified in CIP-002-5, Requirement R1, Part R1.3, shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that collectively address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months.	Not Applicable (Responsible Entity Organizational function)

imagination at work

	R3	Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.	Not Applicable (Responsible Entity Organizational function)
	R4	The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.	Not Applicable (Responsible Entity Organizational function)
CIP-004-5.1 Personnel & Training	R1 – R3	Awareness, Training and Personnel Risk Assessment	Not Applicable (Responsible Entity Organizational function)
	R4	Access Management Program	Not Applicable (Responsible Entity Organizational function)
	R5	Access Revocation	Responsible Entity Organizational function The G500 can help enforce this process thanks to its support for TACACS+ and LDAP, which provides a centralized administration point where users can be revoked. The G500 also supports manually deployed Certificate Revocation Lists to remove a user's access to network IEDs using SSL/TLS.
a	R1.1	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	Responsible Entity Organizational and Project Engineering function. G500 facilitates implementing this requirement by using different NICs.

	R1.2	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	Responsible Entity Organizational and Project Engineering function. G500 facilitates implementing this requirement by using different NICs. The G500 can constitute an EAP. User authentication is possible via login/password or certificates. For central authentication, multifactor authentication is possible with TACACS+RSA SecureID. The G500 can also be connected to an EAP – as desired.
	R1.3	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	G500 facilitates implementing this requirement by using different NICs and an internal rule based and configurable firewall. The G500 will only enable the ports and services configured. The firewall will automatically block all other ports.
	R1.4	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	When used as an EAP, for the purpose of providing access to Cyber Assets, G500 can be configured to require name and certificate-based authentication. Authentication can be based on locally defined user or centrally managed users via LDAP or TACACS+.
	R1.5	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	The G500 logs authentication attempts, connections status, and firewall actions.
	R2.1	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Responsible Entity Project Engineering function. G500 facilitates implementing this requirement by using different NICs and an internal rule based and configurable firewall and RBAC.
	R2.2	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	G500 can be configured to allow remote access sessions using HTTPS (TLS), SSH, and VPN.
	R2.3	Require multi-factor authentication for all Interactive Remote Access sessions	Responsible Entity Project Engineering function. For remote HMI access, G500 assists compliance by using LDAP or TACACS+ authentication which in turn can be configured to require RSA token access in the organization. For Remote Access sessions for the purpose of pass-through EAP connections (“virtual connection”) – the G500 requires user names and keys/certificates.

CIP-006-5 Physical Security of BES Cyber Systems	All	All	Not applicable to G500 – Responsible Entity Organization function. G500 assists in implementing these requirements by providing a configurable real time interface to the systems which monitor Physical Access, using industry standard communication protocols (for e.g.: SNMP, MODBUS, ASCII). Events gathered can be alarmed locally or remotely via email, RSYNC over SSH, SFTP, FTP (push). Event can also be forwarded to a syslog server or a SIEM via syslog protocol.
CIP-007-5 Systems Security Management	R1.1	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	G500 facilitates implementing this requirement by using an internal firewall, rules based and configurable. The G500 will only enable the ports and services associated with the configured functionality. The firewall will automatically block all other ports. Users can further edit and customize the firewall rules as needed and close/open ports according to their needs.
CIP-007-5 Systems Security Management	R1.2	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media.	USB ports can be disabled. Network ports are disabled by default. Front maintenance port which can be disabled by configuration.
CIP-007-5 Systems Security Management	R2.1	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	The GE SDLC includes testing with vulnerability scanners and fuzzers tailored for the G500. Our scanning tools are continuously updated for the latest vulnerabilities and issues and run against our devices. GE PSIRT maintains a registered users list for Cyber Security notifications. The process is setup to send notifications to registered users if a critical vulnerability is identified. Based on severity and exposure of vulnerability details, the assessment of new discovered vulnerabilities is within 30 days. G500 logs all installations of patches and this log is available to administrators.
CIP-007-5 Systems Security Management	R2.2	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	Responsible Entity Organizational function. Aided by the GE process notification of registered users.

CIP-007-5 Systems Security Management	R2.3	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: • Apply the applicable patches; or • Create a dated mitigation plan; or • Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	Responsible Entity Organizational function. Aided by the GE process notification of registered users.
CIP-007-5 Systems Security Management	R2.4	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	Responsible Entity Organizational function.
CIP-007-5 Systems Security Management	R3.1	Deploy method(s) to deter, detect, or prevent malicious code.	Responsible Entity Organizational and Process Engineering function, for e.g. offline scanning of USB FLASH drives used for patching, control electronic access to resources. This is aided by the G500 being based on an embedded computer platform. G500 is built with in-depth security concept (access control, hardening, no backdoors, etc.). Even if an attacker finds a way to inject malicious code in the device, several other mechanisms are there to ensure security: • The device Operating system is a Linux base hardened following security best practices (ex. kernel hardening, privilege separation, etc.) • The Operating System security relies on secured containers which allow isolation between applications. Concerning the Windows hosted configuration tools such as DSAS (DS Agile Studio). We recommend the customer installs antimalware solution based on application whitelisting technology on all PCs.

CIP-007-5 Systems Security Management	R3.2	Mitigate the threat of detected malicious code.	Responsible Entity Organizational and Process Engineering function. The G500 aides by providing logs of all running application processes, with their unique ID and dependencies. The Operating System security relies on secured containers which allow isolation between applications.
CIP-007-5 Systems Security Management	R3.3	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	Responsible Entity Organizational and Process Engineering function. The G500 does not support the major delivery mechanisms of malware targeted for generic operating systems. See R3.1 answer
CIP-007-5 Systems Security Management	R4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts;	The G500 logs successful and failed login attempts, as well as running processes with their application ID.
CIP-007-5 Systems Security Management	R4.1.3	Detected malicious code.	The G500 is an embedded computer platform, using Linux OS. The following major sources of entry of mainstream malware are simply not supported by the G500: • Installable third-party programs using generic tools like apt-get, yum or windows installer • Auto mount and auto-run of programs on a USB stick or CD drive • Opening documents with embedded macros • Receiving emails with attachments • External web browsing • open file shares The Responsible Entity Organizational and Process Engineering should develop procedures to control offline scanning of USB FLASH drives used for G500 patching. Also see R3.1 answer

CIP-007-5 Systems Security Management	R4.2	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	See R3.1 Failure of the event logging subsystem itself cannot be logged by the same failed subsystem; appropriate system architectures can be deployed, where absence of renewed logs present (uploaded) at an Enterprise Level can be detected and alarmed.
CIP-007-5 Systems Security Management	R4.3	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Responsible Entity Organizational and Process Engineering function. Logs in G500 are maintained by size, not by time. G500 log rotate mechanism maintains last 10 user activity log files, each 256 KB of size (2.56 MB maximum); the System Architecture should provision for the G500 to send these logs to an Enterprise Repository for long term availability.
CIP-007-5 Systems Security Management	R4.4	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	Responsible Entity Organizational and Process Engineering function. Logs in G500 are maintained by size, not by time, it is up to the Responsible Entity to review them as needed.
CIP-007-5 Systems Security Management	R5.1	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	All interactive user access to the G500 is subject to authentication, either local or remote (TACACS+, LDAP).
CIP-007-5 Systems Security Management	R5.2	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Responsible Entity Organizational and Process Engineering function. G500 does not have generic accounts that cannot be changed. The following roles exist in G500; a given user can be assigned to a role: • Administrator (full rights) • Supervisor (full access to the HMI) • Operator (can execute commands but nor change configuration) • Observer (can only see data)
CIP-007-5 Systems Security Management	R5.3	Identify individuals who have authorized access to shared accounts.	Responsible Entity Organizational and Process Engineering function. For Local based authentication, the list of accounts is presented in the G500 configuration tools.

CIP-007-5 Systems Security Management	R5.4	Change known default passwords, per Cyber Asset capability.	Responsible Entity Organizational and Process Engineering function. G500 does not have passwords that cannot be changed.
CIP-007-5 Systems Security Management	R5.5	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	G500 complies and exceeds all R5.5 requirements for password complexity when Local based authentication is used. For Remote based authentication (TACAS+, LDAP) – the password complexity requirements must be implemented in the central servers.
CIP-007-5 Systems Security Management	R5.6	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	While the G500 alone doesn’t enforce timely passwords changes, the Responsible Entity can meet this requirement by using centralized user management and procedures enforcing the timely changes.
CIP-007-5 Systems Security Management	R5.7	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or • Generate alerts after a threshold of unsuccessful authentication attempts.	G500 complies to R5.7 requirements.
CIP-008-5 Cyber Security Incident Response	R1.1	One or more processes to identify, classify, and respond to Cyber Security Incidents.	Responsible Entity Organizational function. The G500 provides the necessary logs enabling the Responsible Entity to implement this requirement.

Plan Specifications	R1.2	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	Responsible Entity Organizational function. The G500 provides the necessary logs enabling the Responsible Entity to implement this requirement.
	R1.3	The roles and responsibilities of Cyber Security Incident response groups or individuals.	Responsible Entity Organizational function.
	R1.4	Incident handling procedures for Cyber Security Incidents.	Responsible Entity Organizational function.
	R2.1	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months (…)	Responsible Entity Organizational function.
	R2.2	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	Responsible Entity Organizational function.
	R2.3	Retain records related to Reportable Cyber Security Incidents.	Responsible Entity Organizational function. Logs in G500 are maintained by size, not by time, it is up to the Responsible Entity to retain logs as required.
	R3.1	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response (…)	Responsible Entity Organizational function.
	R3.2	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan (…)	Responsible Entity Organizational function.

CIP-009-5 Recovery Plan Specifications	R1.1	Conditions for activation of the recovery plan(s).	Responsible Entity Organizational function.
	R1.2	Roles and responsibilities of responders.	Responsible Entity Organizational function.
	R1.3	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	Responsible Entity Organizational function. G500 assists compliance via snap-shot images which can be remotely retrieved and restored using DSAS (SFTP & SSH protocol).
	R1.4	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	Responsible Entity Organizational function. G500 assists compliance when using compressed configuration archives with integrity checks in place.
	R1.5	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	Responsible Entity Organizational function. See R1.3
	R2.1	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.	Responsible Entity Organizational function.
	R2.2	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	Responsible Entity Organizational function.

	R2.3	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	Responsible Entity Organizational function.
	R3.1	No later than 90 calendar days after completion of a recovery plan test or actual recovery (...)	Responsible Entity Organizational function.
	R3.2	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan: • 3.2.1. Update the recovery plan; and • 3.2.2. Notify each person or group with a defined role in the recovery plan of the updates.	Responsible Entity Organizational function
CIP-010-1 Configuration Change Management and Vulnerability Assessments	R1.1	Develop a baseline configuration, individually or by group, which shall include the following items: • Operating system(s) (including version) or firmware where no independent operating system exists; • Any commercially available or open-source application software (including version) intentionally installed; • Any custom software installed; • Any logical network accessible ports; and • 1.1.5. Any security patches applied.	Responsible Entity Organizational Function. G500 assists compliance by allowing users to create snap-shots of the configurations used via DSAS.
	R1.2	Authorize and document changes that deviate from the existing baseline configuration.	Responsible Entity Organizational Function. DSAS Detailed Config Compare utility can help with the process based on the configurations.

	R1.3	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	Responsible Entity Organizational Function and Process.
	R1.4	For a change that deviates from the existing baseline configuration: • 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; • 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and • 1.4.3. Document the results of the verification.	Responsible Entity Organizational and Engineering Function and Process. Users should engage in necessary testing and qualification processes before installing or changing the G500 within a live BES Cyber System. G500 assists compliance by providing all configurations in XML format, which can be easily compared (via DSAS Detailed Config Compare utility).
	R1.5.1	Where technically feasible, for each change that deviates from the existing baseline configuration: • 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected;	Responsible Entity Organizational and Engineering Function and Process. Users should engage in necessary testing and qualification processes before installing or changing the G500 within a live BES Cyber System.
	R1.5.2	Where technically feasible, for each change that deviates from the existing baseline configuration: • 1.5.2. Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	Responsible Entity Organizational and Engineering Function and Process. Users should engage in necessary testing and qualification processes before installing or changing the G500 within a live BES Cyber System.

	R2.1	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	Responsible Entity Organizational and Engineering Function and Process. G500 assists compliance by providing all configurations in XML format, which can be easily compared (via DSAS Detailed Config Compare utility).
	R3.1	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Responsible Entity Organizational and Engineering Function and Process.
	R3.2	Where technically feasible, at least once every 36 calendar months: • 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and • 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	Responsible Entity Organizational and Engineering Function and Process.
	R3.3	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset.	Responsible Entity Organizational and Engineering Function and Process.

	R3.4	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	Responsible Entity Organizational and Engineering Function and Process.
CIP-011-1 Cyber Security — Information Protection	R1.1	Method(s) to identify information that meets the definition of BES Cyber System Information.	Responsible Entity Organizational and Engineering Function and Process. Based on its end user application, the G500 can be a Medium or High Impact asset.
	R1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Responsible Entity Organizational and Engineering Function and Process. To further assist, the G500 offline configuration tool (DSAS) provides integrity validation for configuration archives and snapshots (when a strong password is used).
	R2	R2.1: Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the “Applicable Systems” column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media. R2.2: Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Since the configuration and sensitive date exist in the G500’s removable compact flash cards, it is recommended that these cards be removed before disposing the G500 or sending it for repairs. It is the Responsible Entity’s responsibility to protect these cards and/or destroy the contained information accordingly.

Frequently Asked Questions (G500)

The following NERC CIP-007-5: Frequent Asked Questions, are applicable to the G500.

CIP-007-5 R1 – Ports and Services

Q : R1a - Provide a list of factory default open ports – tcp and udp

A : Please refer to the following table for complete list of ports. Factory default open ports are indicated by "**Yes**" from the "Enabled by default?" column.

Port Numbers	TCP/UDP	Enabled by default ?	Used for
443	TCP	Yes	Sync to/from, Online Editor, PETC, Remote runtime HMI.
22	TCP	Yes	Snapshot save/restore, shell access to gateway, file transfer with Gateway.
922	TCP	No	Emergency administrator access, open only when remote authentication configured.
80, 8081	TCP	Yes	Settings GUI.
123	TCP	No	NTP, if configured.
Configurable, default 502	TCP	No	MODBUS, if configured.
Configurable, default 2404	TCP	No	IEC60870-5-104, if configured.
514	UDP	No	Rsyslog, if configured.
10514	TCP	No	Rsyslog, if configured.
Configurable, default 20000	TCP/ UDP	No	DNP, if configured.
Configurable, default 8001 – 8020	TCP	No	Pass-through or terminal server, if configured.
Configurable	TCP	No	TLS tunnel for pass through, terminal server or secure connection relay, if configured.
54000	TCP	No	LogicLinx, if configured.
162	UDP	No	SNMP, if configured.
Configurable, default 1194	UDP	No	OpenVPN, if configured.
51000	TCP	No	Hot Standby Sync Service, if Hot Standby configured.
51001	TCP	No	Hot/Warm Standby Heart Beat, if Hot/Warm-Standby Configured.
51003	TCP	No	Standby pointing to active tunnel, if configured.
51194, 51195	TCP	No	Hot/Warm Standby Tunnel, if Hot/Warm-Standby Configured.

Q : R1b - Can these ports be closed via firmware or software?

A : Yes, by configuring with custom firewall rules.

Q : R1c - Can new ports be opened via firmware or software?

A : Yes, by configuring any LAN applications, Rsyslog Service, Secure Connection Relay, Terminal Server, SNMP, OpenVPN, or NTP, the associated ports will be opened.

CIP-007-5 R2 – Security Patch Management

Q : R2a - Are automated security update notifications available from the vendor via email?

A : GE Multilin™ maintains a registered users list for Cyber Security notifications. The process is setup to send notifications to registered users if a critical vulnerability is identified.

Q : Can GE provide periodic updates for the G500 that would bring software such as the operating system, web server, and database up to their current versions?

A : G500 updates are currently planned to be provided on an as-needed basis. Patch updates are signed, and signed firmware updates are under development. In the meantime, the method for at least G500 firmware v1.1 is to update the whole firmware as a single image with the configuration being backed up, upgraded and restored by the desktop software.

CIP-007-5 R3 – Malicious software prevention

Q : R3a - Does the device support anti-malware tools?

A : No, as this is not currently technically feasible, as well as the device does not run a generic OS but a tailored RTOS that is not designed to load or execute 3rd party software components or programs.

CIP-007-5 R4 – Security Status Monitoring

Q : R4a - Does the device provide support for automated security status monitoring tools, specifically for monitoring system events related to cyber security (example, syslog)?

A : Yes, the G500 logs events in SOEs can retrieve any syslog files from connected IEDs.

Q : R4b - Can the device log events, especially security related events?

A : Yes, the G500 logs successful and unsuccessful login attempts, any use of sudo, password change, SSH sessions information, and more.

Q : R4c - Can the device detect a security incident?

A : No, the G500 relies on a Security Event Manager software package to perform alerts of a security incident.

Q : R4d - Can the device send an alert upon detecting a security incident?

A : No, the G500 relies on a Security Event Manager software package to perform alerts of a security incident.

CIP-007-3 R5 – Account Management

Q : R5a - Can the device be accessed remotely via the network?

A : Yes, if configured.

Q : R5b - If yes, does the access method use login accounts?

A : Yes, the access method uses both local accounts and remote accounts via LDAP or TACAC server.

Q : R5c - Provide a list of factory default accounts and their access privileges (e.g. administrator, individual, shared, read-only, read-write)?

A : Factory default User account/Username: **defadmin**; Access privilege: **administrator**. This is an administrator account that is used only for initial IP address and admin user setup. As soon as an admin account is created and logged into, this 'defadmin' account is automatically removed.

Serial default User account/Username: **root**; Access privilege: **administrator**. This is present on all Linux computers, and the expectation is that the Customer will change this to a password of their choosing.

Predix Edge Console default User/Username: **admin**; Access privilege: **administrator**. This is present for future expansion. A default Admin user and password exist, and the expectation is that the Customer will change the password to something of their choosing.

Q : R5d - Can new user accounts be created in addition to the factory default ones?

A : Yes.

Q : R5e - Can the privileges of the user accounts be changed for both – factory default and newly created ones?

A : No, the factory default user account privileges cannot be changed. The newly created account privileges can be changed for HMI use.

Q : R5f - Does the access require passwords?

A : Yes, access to the G500 always requires password.

Q : R5g - If yes, does the G500 enforce the password to have the minimum number of characters (combination of alpha, numeric, and special)?

A : Yes, the password must be minimum 8 characters and have at least one number and at least one special character.

Q : R5h - Can the device support a user access log?

A : Yes, the G500 support local SOE log, which can be accessed remotely, as well as ability to retrieve any Syslog logs from any connected device.

Q : R5i - If yes, can the user access log be stored in the device for at least 90 days for auditing purposes?

A : Yes, the local user access log can be configured to hold enough records for normal account activity over a period of 90 days (e.g. 10,000 records).

In addition – SNMP related questions

Q : Does the device support SNMP?

A : Yes, as an SNMP client only.

Product Support

If you need help with any aspect of your GE Grid Solutions product, you can:

- Access the GE Grid Solutions Web site
- Search the GE Grid Solutions Technical Support library
- Contact GE Grid Solutions Technical Support

GE Grid Solutions Web Site

The GE Grid Solutions Web site provides fast access to technical information, such as manuals, release notes and knowledge base topics.

Visit us on the Web at: http://www.gegridsolutions.com

GE Grid Solutions Substation Automation Technical Support Library

This site serves as a document repository for post-sales requests. To get access to the Technical Support Web site, go to: http://sc.ge.com/*SASTechSupport

Contact GE Grid Solutions Technical Support

GE Grid Solutions Technical Support is open 24 hours a day, seven days a week for you to talk directly to a GE representative.

In the U.S. and Canada, call toll-free: 1 800 547 8629.

International customers call: +1 905 927 7070

Or send an e-mail to: multilin.tech@ge.com

Copyright Notice

Trademark Notice

Document Revision History

Version	Revision	Date	Author	Change Description
1.00	0	Sept 30th, 2019	E. Nasi	Initial Release
1.10	0	March 3rd, 2020	N. Ajwad	Added FAQ section.