**Supply Chain and External Dependencies Management**

Describe how you perform security assessments of third-party companies with which you share data (i.e., hosting providers, cloud services, PaaS, IaaS, SaaS, etc.). Provide a summary of your practices and/or controls that assure the third party will be subject to the appropriate standards regarding security, service recoverability, and confidentiality. Ensure that all elements are clearly stated in your response.

- The Third Party Management Policy says “proper due diligence shall be performed prior to provisioning access or engaging in processing activities.”

Describe or provide references to your third-party risk management strategy or provide additional information that may help analysts better understand your environment and how it relates to third-party solutions. Robust answers improve the quality and efficiency of the security assessment process.

- I have submitted a Third Party Management Policy, let me know if you need me to send it again.

Does your policy include a requirement to implement processes designed to ensure that all agreements or contracts with your service provider(s) contain specific clauses to protect data or systems when accessed, processed, or stored by its third-party suppliers/service providers?

- The Third Party Management Policy does.

Do you have an established program that ensures the storage security at your site (e.g., chain of custody)? Please describe this program and how it is maintained.

- The GPA Confidential Data Policy says that we do this but does not provide specifics on how.

Do you have a process by which you confirm the source of software downloads and the integrity of the software downloaded prior to use in your environment? Please describe this process.

- Not that I’m aware of.

Do you have a process by which you verify and provide documentation that procured products (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to delivery? Please describe this process.

- Not that I’m aware of.

Have you established and do you maintain a program that ensures secure transport of assets based on risk need (e.g., chain of custody, tracking, enhanced packaging)? Please describe this process.

- The GPA Confidential Data Policy has this as a requirement but does not outline the steps.

Have you established and do you maintain a security management program that validates the authenticity and origin of third-party hardware, firmware, and software including open source code? Please describe or provide a reference to/copy of this policy.

- There is a GPA Management of Open-Source Code Procedures policy, but it does not mention validating authenticity or origin of third party code.

Do you have a process by which you will notify purchaser when production and/or operation of products and/or services changes to another supplier or location?

- Not that I’m aware of.

Do you document country of source for all components of any product provided to your customers?

- Not that I’m aware of.

Does your information protection program include safeguards and notifications regarding the release of data to third parties? Please describe this aspect of your program in adequate detail.

- Third Party Management Policy - “Grid Protection Alliance shall not share or transmit Confidential data to a third-party without first performing a third-party risk assessment and fully executing a written contract, statement of work or service agreement which describes expected service levels and any specific information security requirements.”

Do you have a process by which you identify and document vulnerabilities in third-party product(s) used by you in the production or delivery of your product(s) to your customers, including the utility? Do you notify the utility and your other customers of these vulnerabilities throughout the lifecycle of the product(s) or service(s) provided by you? Please describe this process, including timeframe for a method by which notification is provided.

- Not that I’m aware of.

Do you require your applicable third parties to have a designated privacy function responsible for its privacy policy and program as it relates to Privacy Data?

- Yes.

Provide a brief description for each of these third-party entities explaining the types of utility data they have access to and why each of these third parties REQUIRES access to utility data.

- I believe an Acceptable Use Policy should cover this.

Do you have legal agreements (i.e., contracts) in place with these third parties that address liability in the event of a data breach? Provide a sufficient description and/or details for each legal agreement in place.

- The Third Party Management Policy states “Vendors must promptly notify Grid Protection Alliance of any actual or suspected security incidents, breaches, or unauthorized access involving Grid Protection Alliance data or systems. The contract will specify a required notification time frame and require cooperation in any incident investigation or response.”

**Workforce Management**

Do you perform background screenings or multi-state background checks, including seven-year criminal background checks, on all personnel, including employees, contractors, and subcontractors, prior to their first day of work? Summarize background check practices including level (e.g. seven-year background checks) and list of any exempted employees or contactors due to restrictions by country of employment.

- The Human Resource Security Policy states “Background verification checks on Grid Protection Alliance personnel shall be carried out in accordance with relevant laws, regulations, and shall be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. All third-parties with technical privileged or administrative access to Grid Protection Alliance production systems or networks are subject to a background check or requirement to provide evidence of an acceptable background, based on their level of access and the perceived risk to Grid Protection Alliance.” I don’t believe this is done currently though.

Do you perform recurring background checks for personnel on a periodic basis after initial hire date? Provide frequency that supplier's process requires and list of any exempted employees or contactors due to the personnel's area of responsibility or restrictions by country of employment.

- No.

Does your personnel vetting process allow you to share background check criteria and/or the process itself with utility for confirmation of process or verification of sampled employees?

- No.

"Please describe your staff offboarding procedures, including the following:

* timeframe for termination of system and physical access
* timeframe for notifying customers of termination of personnel
* cases in which personnel will no longer need physical or logical access to the utility's sites or systems."

- The offboarding process is incomplete and does not currently require timeframes, but it does include revoking access to systems.

For access within supplier's system, does supplier have implemented internal controls to ensure it revokes access when an individual no longer requires access due to change in employment status or job duties?

- Access Control Policy: “The access rights of all users shall be promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role.”

For access within supplier's system, does supplier revoke access when an individual no longer requires access due to change in employment status or job duties?

- Access Control Policy: “The access rights of all users shall be promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role.”

For access within supplier's system functioning as a BCSI repository for utility data, has supplier implemented procedures to revoke access within 24 hours when any individual no longer requires access due to change in employment status or job duties?

- Access Control Policy: “The access rights of all users shall be promptly removed upon termination of their employment or contract, or when rights are no longer needed due to a change in job function or role. The maximum allowable time period for access termination is 24 business hours.”

Do you have a documented program for secure product development, including applying security controls and secure coding techniques, within the system development life cycle? Describe your secure product development program.

- There is a Secure Development Policy which has not been started in Vanta yet.

Do you have a training and awareness program for your application developers to ensure they are aware of current secure coding techniques and security risks in application development? Summarize your securing coding training and state how frequently employees are required to undergo this training.

- In the Human Resource Security Policy there is a section on Information Security Awareness, Education, and Training, but it does not mention secure coding techniques.

Do you have a process by which you determine whether any employee, contractor, or subcontractor appears on any list of prohibited persons maintained by any government authority ("Prohibited Lists"), including but not limited to the list of "Specially Designated Nationals and Other Blocked Persons" maintained by the United States Department of Treasury, and the "Denied Persons List" maintained by the Bureau of Industry & Security?

- No.

Which groups of staff (individual contractors and full-time) have access to utility data? How many staff would have logical access to our data? What is your policy on providing notification if/when rotating staff will handle utility data/projects?

- Access Control Policy: “Grid Protection Alliance shall ensure that the allocation and use of privileged access rights are restricted and managed judiciously. The objective is to ensure that only authorized users, software components, and services are granted privileged access rights.” I’m not sure if there is a policy that mentions notification.

Do you require employees to have a completed agreement and review information security policies including, but not limited to, an Acceptable Use policy or equivalent? Summarize the required agreements and reviewed policies.

- There is an Acceptable Use Policy listed in Vanta, and one part of Vanta’s requirements is that all employees have completed all security training.

Is security awareness and privacy training mandatory for all employees at least annually? Summarize your security awareness and privacy training content and state how frequently employees are required to undergo security awareness training.

- Not currently, although Vanta has a section on the roadmap to get this started.

**Identity and Access Management**

Describe your authentication and authorization processes.

- To be mentioned in the Access Control Policy and Acceptable Use Policy. We use MFA for all internal systems and for access to sensitive data through Duo Security or authenticator apps.

Do you establish and maintain an identity and access management program that ensures sustainable, secure product manufacturing and development? Please provide a high-level description of the major components of this program.

- Not that I’m aware of.

Do you require approval for access based on need for all personnel with access to your assets and/or facilities? Please describe the approval process.

- Yes, appropriate access is granted on hire or on new projects.

Do you maintain a list of all individuals with access to your assets, systems, networks, information, and/or facilities including an access log of each sign in/out?

- The Access Control Policy has an appendix with an access matrix that can be edited/updated. Wazuh will be able to track all access logs.

Do you maintain an access list of all individuals with access to utility's assets, information and facilities?

- The Access Control Policy includes an access matrix in the appendix (Currently just an example matrix, needs updating)

Do you conduct an annual review of all individuals' access to your assets, systems, networks, information, and facilities to ensure access is still required?

- Access Control Policy: “Administrators shall perform access rights reviews of user, administrator, and service accounts on a quarterly basis to verify that user access is limited to systems that are required for their job function. Access reviews shall be documented. Access reviews may include group membership as well as evaluations of any specific or exception-based permission. Access rights shall also be reviewed as part of any job role change, including promotion, demotion, or transfer within the company.”

Do you conduct an annual review of all individuals' access to the utility's assets, systems, networks, information, and facilities for which you provision and deprovision access?

- Access Control Policy: “Administrators shall perform access rights reviews of user, administrator, and service accounts on a quarterly basis to verify that user access is limited to systems that are required for their job function. Access reviews shall be documented. Access reviews may include group membership as well as evaluations of any specific or exception-based permission. Access rights shall also be reviewed as part of any job role change, including promotion, demotion, or transfer within the company.”

Do you have a policy that prohibits the use of shared accounts and/or shared credentials? Describe your policy for preventing the use of shared accounts and shared credentials.

- This should be covered in the Acceptable Use Policy

Please describe your process for administering production systems (e.g., multi-factor authentication, jump hosts, etc.).

- This takes place during onboarding or any time new access is required. Documentation is updated accordingly.

Describe or provide a reference that details how administrator access is handled (e.g., provisioning, principle of least privilege, deprovisioning, etc.). Ensure that all parts of the question are clearly stated in your response.

- I would guess this would be covered in either the Acceptable Use Policy or the Access Control Policy.

Do you have a process or policy for administering administrative accounts? Describe or attach your policy or process.

- Not specifically for administrative accounts. See Access Control Policy.

Do you have process(es) and procedure(s) documented, and currently followed, that require a review and update of the access-list(s) for privileged accounts? Provide a brief summary and the review interval.

- Access Control Policy: “Administrators shall perform access rights reviews of user, administrator, and service accounts on a quarterly basis to verify that user access is limited to systems that are required for their job function. Access reviews shall be documented.”

**Cybersecurity Program Management**

Do you have a business continuity plan (BCP) to support ongoing operations of your systems and scope of equipment and/or services provided to the utility? Provide a reference to your BCP and supporting documentation or submit it along with this fully-populated questionnaire. Please also describe how you ensure data availability in the event of the loss of systems or facilities.

*I have a BCP from Christoph, I’m just including this so the next couple of questions make sense.*

Are all components of the BCP reviewed at least annually and updated as needed to reflect change? Describe your BCP component review strategy.

- The current BCP does not mention annual review of components.

Has your BCP been tested in the last year? State the date of your last BCP test.

- “A disaster recovery test, including a test of backup restoration processes, shall be performed on an annual basis.” I’m not sure the date of the last one.

Do you have a media handling process (that is documented and currently implemented) including end-of-life, repurposing, and data sanitization procedures? Provide details of these procedures (link or attached).

- Asset Management Policy: “Company devices and media that stored or processed confidential data shall be securely disposed of when no longer needed. Data must be erased prior to disposal or reuse, using an approved technology in order to ensure that data is not recoverable. Or a Certificate of Destruction (COD) must be obtained for devices destroyed by a third-party service.”

Does your information protection program include secure deletion (e.g., degaussing/cryptographic wiping) or destruction of sensitive data, including archived or backed-up data? Please provide a brief description of this process.

- Yes, as per the Asset Management Policy, noted in the above answer.

Do you have third-party assessment(s) and/or certification(s) you have conducted to assess your cybersecurity practices? If yes, please describe the assessment or certification, date last completed, and frequency of re-assessment. Provide the findings reports from third-party verifications conducted for cybersecurity frameworks (provide the two most recent reports for each cybersecurity framework).

- I believe the last pen test was 2 years ago? This is where we would include SOC 2 audit results.

Do you establish and maintain a security program for your environment, including implemented processes to approve software, patches, and firmware prior to installation, as well as to verify the integrity and authenticity of the software, patches and firmware relevant to any technologies or equipment used in the development, manufacturing, testing, assembly, and distribution of the product(s) or service(s)? Please describe this program in adequate detail.

- This may be addressed in the Secure Development Policy or Operations Security Policy.

Do you have and follow documented operating procedures and technological controls to ensure the effective management, operation, integrity, and security of information systems and data? Please summarize the technical controls.

- This may be included in the Operations Security Policy.

Is there a defined problem/issue escalation plan in your BCP for impacted clients of the computing system? Summarize your defined problem/issue escalation plan contained in your BCP.

- The BCP states: “Executive staff and senior managers should be notified of any disaster affecting Grid Protection Alliance facilities or operations.”

Do you have a disaster recovery plan (DRP) for your computing systems? Describe how your DRP is validated and exercised.

- Yes, it is included in the BCP.

Do you have an overarching information security policy or procedure that can be shared with utility clients? Provide links to these documents or attach them. Include the responsible party for your information security program and the size of your security staff.

- There is an Information Security Policy/Acceptable Use Policy in Vanta that is incomplete.

At the completion of this contract, will measures be taken to ensure data is deleted securely, or managed as per the agreed upon contract? Describe how data will be returned to the utility and in what format will it be presented, as well as how data will be securely deleted from your systems.

- Data Management Policy: “Data classified as restricted or confidential shall be securely deleted when no longer needed. Grid Protection Alliance shall assess the data and disposal practices of third-party vendors in accordance with the Third-Party Management Policy. Only third-parties who meet Grid Protection Alliance requirements for secure data disposal shall be used for storage and processing of restricted or confidential data.”

Do you have data retention policies that are relevant to this engagement? Provide a reference to the requested documents or attach them.

- Data Management Policy: “Grid Protection Alliance shall retain data as long as the company has a need for its use, or to meet regulatory or contractual requirements. Once data is no longer needed, it shall be securely disposed of or archived. Data owners, in consultation with legal counsel, may determine retention periods for their data.”

Are ownership rights to all data, inputs, outputs, and metadata retained by the utility? Provide reference to or attach your data ownership documentation.

- I don’t believe we have any data ownership documentation.

Do procedures exist to ensure that retention and destruction of data meets established business and regulatory requirements? Provide a general summary of your long-term data retention strategy.

- Data Management Policy: “Grid Protection Alliance shall retain data as long as the company has a need for its use, or to meet regulatory or contractual requirements. Once data is no longer needed, it shall be securely disposed of or archived. Data owners, in consultation with legal counsel, may determine retention periods for their data.” and also “Data classified as restricted or confidential shall be securely deleted when no longer needed. Grid Protection Alliance shall assess the data and disposal practices of third-party vendors in accordance with the Third-Party Management Policy. Only third-parties who meet Grid Protection Alliance requirements for secure data disposal shall be used for storage and processing of restricted or confidential data. Grid Protection Alliance shall ensure that all restricted and confidential data is securely deleted from company devices prior to, or at the time of, disposal. Confidential and Restricted hardcopy materials shall be shredded or otherwise disposed of using a secure method.”

Are processes in place to handle utility data in both a CUI and a CEII compliant manner? Describe how compliance is integrated into your process and procedures.

- These requirements are outlined in the Data Management Policy.

Do you maintain an asset management program that requires an inventory of IT and OT hardware, software, information assets (e.g., databases)?

- Yes.

**Change and Configuration Management**

Do you have a documented and currently followed change management process (CMP) for the systems and networks under your control? Summarize your current change management process.

- No.

Does your organization have policies and/or procedures to ensure that only application software verifiable as authorized, tested, and approved for production is placed into production and/or released for client use? Describe how this is accomplished within your environment.

- This might be handled in the Secure Development Policy. (Not started yet)

Do you have a process to assess and apply security patches in your environment within a predetermined timeframe? Please provide the number of days to complete the assessment and implementation.

- Not within a predetermined time frame. The vulnerability scanner and Wazuh provide information on necessary patches. GPA Software Update, Patch, and Configuration Management Policy: “GPA monitors all IT systems on a continuous basis in accordance with its policies and procedures. In addition, GPA may use automated systems to identify the state of IT systems regarding flaw remediation. Employees assigned to maintaining central infrastructure must ensure any identified flaw remediation actions are taken in a timely fashion.”

Do you have an implemented system configuration management process (e.g., secure "gold" images, etc.)? Summarize your implemented system configuration management process.

- GPA Software Update, Patch, and Configuration Management Policy: “Any employees assigned to maintaining central infrastructure must:

• Determine the types of changes to the equipment that are configuration-controlled.

• Review proposed configuration-controlled changes to the equipment and approve or

disapprove such changes with explicit consideration for security impact analyses.

• Document configuration change decisions associated with the equipment.

• Implement approved configuration-controlled changes to the equipment.

• Retain records of configuration-controlled changes to the information system for at

least six (6) months.

• Test, validate, and document changes to the equipment before implementing the

changes on the operational system.

• Ensure any change to the configuration does not adversely impact GPA’s operational

processes or cyber security processes.”

Do you have a systems management and configuration strategy that encompasses servers, appliances, and mobile devices (company and employee owned)? Summarize your systems management and configuration strategy.

- GPA Software Update, Patch, and Configuration Management Policy: “Any employees assigned to maintaining central infrastructure must:

• Ensure the baseline configuration of the equipment or software is recorded in GPA’s IT

procedures and information spreadsheet.

• Regularly review and update the baseline configuration record.”

- Also refer to the previous question’s bulleted list. No strategy in place for mobile devices.

Provide a general overview of the process used for your CMP. If you follow a specific industry standard or practice, provide a reference to it or attach additional documentation. Ensure that all parts are clearly stated in your response.

- GPA Software Update, Patch, and Configuration Management Policy.

Do you have policy(ies) and procedure(s), currently implemented, managing how critical patches are released and/or applied to all systems and applications? Please summarize the policy and procedure(s) managing how critical patches are applied to systems and applications and provide a copy.

- No. There is a GPA Problem Notification Process Procedure, however it does not outline how patches are applied, just that problems will be posted and users notified.

Do you have policy(ies) and procedure(s), currently implemented, guiding how security risks are mitigated until patches can be applied? Summarize the policy and procedure(s) guiding risk mitigation practices before critical patches can be applied and provide a copy if available.

- No.

Do you have a documented policy for firewall change requests? Please describe the policy, including required approvals, for firewall change requests.

- No.

**Cybersecurity Tools & Architecture**

Is appropriate segregation of duties maintained among those requesting, approving, and provisioning access? Please describe how this is accomplished, including the process by which it is ensure that access has been approved before it is provisioned.

- Yes. Access Control Policy: “Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of Grid Protection Alliance assets. When provisioning access, care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered when determining access levels for individuals and groups.”

Are you utilizing a web application firewall (WAF)? Describe how and where WAFs are currently implemented in your environment.

- I’d assume so? I’m not sure of the implementation.

Are you utilizing a stateful packet inspection (SPI) firewall? Describe how and where SPI firewalls are currently implemented in your environment.

- I’m not sure.

Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?

- We are working on this with Wazuh.

Are development environments and systems separate or segmented from the main corporate network and any other networks? Please describe how the development environments/systems are isolated.

- Yes. According to the network diagram, Webhost01 and Webhost02 are in the DMZ.

Do you have controls for preventing and responding to denial of service (DOS) and distributed denial of service (DDoS) attacks?

- No.

**Event and Incident Response**

Does your company have a Cyber Security Incident response plan/process, including when notification would be provided to purchaser? Please describe your Cyber Security Incident response process, including when notification would be made to purchaser.

- This should be outlined in the Incident Response Plan. (Not started yet)

Does your Cyber Security Incident response plan contain a requirement to notify purchasers of the impacted products or services within 24 hours of initiation of your plan?

- It hasn’t been started yet, but is likely included.

Do you have a process to notify purchasers of any supplier-identified cyber or physical security incidents related to your products or services that could pose risk to the utility?

- No.

Does your Cyber Security Incident response plan include a requirement to perform an after-action review, demonstrate corrective actions (e.g., lessons learned), and update your plan accordingly?

- The plan hasn’t been started yet, although this would presumably be included.

Do you have a process through which you recommend actions to be taken by you and/or purchaser on a purchaser-controlled system to reduce the risk of recurrence of the same or similar security incident, including, as appropriate, the provision of action plans and mitigating controls? Please describe this process.

- This might be part of the Incident Response Plan.

Do you have a program through which you regularly exercise your incident response plan and make corrective actions based on issues identified during the exercise or during actual activation of the plan? If response plan is not exercised on an annual basis, please provide frequency.

- No.

Do you review and update your Cyber Security Incident response plan at least annually? If response plan is not reviewed on an annual basis, please provide frequency.

- No.

Have you taken appropriate action in response to assessment(s) of your Cyber Security Incident response plan/process?

- No current plan.

Does your Cyber Security Incident response plan contain clear roles and responsibilities that include coordination of responses to your purchaser(s)?

- This will likely be covered by the Incident Response Plan, once it is completed.

Does your Cyber Security Incident response plan contain steps to identify, contain, eradicate, and recover?

- It presumably will, once completed.

Do you monitor for intrusions on a 24x7x365 basis with 24x7 response and evaluation? What type of system do you use (network-based, host-based, etc.)?

- Wazuh alerting should help with this, once fully configured.

Do you receive and take action on alerts in real time?

- Wazuh will manage all required alerts once fully configured.

**Risk Management**

Does your organization have physical security controls and policies in place? Provide a copy of your physical security controls and policies along with this document (link or attached).

- Yes. The building and the server room require different authorized keys/badges. This will be outlined in the Physical Security Policy, once it is completed.

Do you use any open source code or freeware/shareware in the subject application? List open source code or freeware/shareware utilized, including frameworks. Describe how you verify integrity and maintain this code, including monitoring for vulnerabilities and deploying patches.

*I don’t expect you to answer this one fully, but if an open source policy is part of SOC2, or Vanta has something relevant we can work off of policy-wise, that would be helpful.*

- There is a GPA Management of Open-Source Code Procedure, which states that all submitted code from any source must be reviewed, but it doesn’t mention maintenance or vulnerability monitoring/patch deployment.

Do you have a process through which you investigate whether computer viruses or malware are present in any software or patches before providing such software or patches?

- This might be covered in the Secure Development Policy. (Not started yet)

Do you have the ability to send automated notifications of and respond to software, patches, and firmware integrity violations?

- I believe Wazuh can be configured to do this.

Do you have a process to monitor industry threat and information sharing entities (e.g., US-CERT, National Vulnerability Database, CISA-AIS)?

- No.

Do you establish and maintain a security program for the product(s) or service(s) being purchased, including implemented processes to verify the integrity and authenticity of the software, patches, and firmware relevant to the product(s) or service(s) being delivered to the utility? Please describe this program.

- No.

Do you use a secure central software repository after software, patches, and firmware authenticity and integrity have been validated, so that authenticity and integrity checks do not need to be performed before each installation?

- Yes.

Do you have a process through which you ensure that products provided by you are not required to reside on out-of-date or out-of-support technologies?

- This might be addressed in the Secure Development Policy. (Not started yet)

Have you implemented processes designed to ensure all of your network connections and devices are adequately tracked, managed, and controlled to protect against threats and to maintain security for the systems and applications using the network?

- Wazuh logging/alerting should be able to handle this.

Have you implemented security controls for the use of devices that access entity's utility's system (e.g., mobile, laptop, non-company devices)? Please describe these controls.

*This is Stephen’s equipment…I don’t know if this is on us or them since he accesses their systems remotely and it’s not him accessing GPA-owned systems.*

- I’m assuming this would just mean his equipment has authentication controls like username/password, perhaps MFA, etc, so I would say yes.

Upon deployment of a new asset, are privileged accounts removed, disabled, or renamed?

- If this refers to changing default usernames and passwords, then I would assume so.

Do you have up-to-date antimalware on all end nodes? Please describe how the antimalware is maintained and kept up-to-date.

- This would probably be addressed in the Information Security Policy. (Not yet started)

In addition to anti-virus, do you have other endpoint protection on your devices? Please describe your endpoint protection strategy.

- Firewalls, Wazuh will provide Extended Detection and Response (XDR) capabilities.

Do you have a risk management policy, procedure, or program? Describe your risk management program, including how you manage supply chain risk. Describe or attach any written policies or procedures. Please indication the frequency at which this policy is reviewed and updated.

- Yes, Risk Management Policy: “Grid Protection Alliance has developed processes to identify those risks that will hinder the achievement of its strategic and operational objectives. Grid Protection Alliance will therefore ensure that it has in place the means to identify, analyze, control and monitor the strategic and operational risks it faces using this risk management policy based on best practices.” And: “Risks are assessed and ranked according to their impact and their likelihood of occurrence. An internal Risk Assessment will be performed at least annually and shall take into consideration the results of any technical vulnerability management activities performed in accordance with the Operations Security Policy.” Third-Party Management Policy: “Grid Protection Alliance will consider and assess risk associated with suppliers and the technology supply chain. Where warranted, agreements with suppliers shall include requirements to address the relevant information security risks associated with information and communications technology services and the product supply chain.”

Does your cybersecurity program conform with a specific industry standard security framework (e.g., NIST Cybersecurity Framework, ISO 27001, etc.)? Please provide any currently effective certifications.

- Not entirely, although the risk assessment I did followed NIST standards.

Is your cybersecurity program compliant with FISMA standards? Or, in the case of products configured by the utility client, do your products include features and capabilities that are in line with FISMA standards?

- Not that I’m aware of.

Are employees allowed to take utility's data out of the computing system in any form? Provide a detailed summary outlining the security controls implemented to protect the Utility’s data.

- I would assume they are not allowed?

Are there any OS (e.g., servers, PCs, switches, routers, etc.) that are not currently supported? Describe all operating systems that are not currently supported, why they still need to be used (i.e. why they cannot be updated), and methods utilized to secure and maintain them.

- Yes. Windows Server 2012, and Ubuntu 20.04. Buildbot has a migration plan in place.

Are information security principles designed into the product lifecycle? Summarize the information security principles designed into the product lifecycle and how they are integrated.

- This is probably addressed in the Information Security Policy. (Not yet started)

**Vulnerability Management**

Are applications running on your computing systems scanned externally and internally for vulnerabilities on a recurring basis? Describe your external application vulnerability scanning strategy and provide when the last assessment was performed.

- A vulnerability scanner has been attached to Vanta, I’m not sure how often it runs.

Do you have a process or program through which you notify purchasers of vulnerabilities and/or material defects and remediations of those items in the product(s) and service(s) supplied by you to them throughout the lifecycle of the product or services provided, to include any vulnerabilities identified and unresolved prior to deployment of product(s) in the customer's environment?

- I would assume so?

Do you notify the utility of any vulnerabilities in your product(s) or service(s) in a timely manner that does not increase threat vectors (e.g., security patch is available or vulnerability is publicly known or imminent to be released publicly)? Please describe in adequate detail, including timeframe for notification.

- This is potentially covered in the Incident Response Plan.

Do you have a process to remediate any security risks identified by purchaser, their representative, or any industry-recognized vulnerability research or assessment organization within a pre-negotiated timeframe? Describe your process to remediate security risks identified and provide timeframe.

- Yes, the Risk Management Policy details that we will either mitigate, accept, transfer, or avoid any risks identified. No timeframe is included.

Do you have secure system hardening guidelines and procedures for products developed or provided by you to purchaser?

- This may be in the Secure Development Policy. (Not started yet)

Do you allow third parties to perform security testing of your systems and/or application provided that testing is performed at a mutually agreed upon time and date? Provide reference to the process or procedure to setup security testing times and scopes.

- We will need annual penetration testing. I believe the last one was 2 years ago.

Do you have software testing processes (dynamic or static) that are established and followed? Describe testing processes, including but not limited to, development of test plans, personnel involved in the testing process, and authorized individual accountable for approval and certification of test results.

- This is likely included in the Secure Development Policy. (Not started yet)

Do you have a documented systems development life cycle (SDLC)? Describe or provide a reference to/attach your system development life cycle methodology including your environments, version control, and change management (if not already covered in the Change Management section).

- This is likely included in the Secure Development Policy. (Not started yet)

Are all code artifacts run through automated validation of production-readiness?

- I would assume so?

Have your systems undergone penetration testing (internal or by third party)? Please provide information on the penetration testing (i.e., when was the test conducted, key findings, etc.).

- Yes, I believe the last one was 2 years ago by a third party.

POLICIES WE NEED:

* Secure Development Policy
* Operations Security Policy
* Physical Security Policy
* Information Security Policy (AUP)
* Incident Response Plan