## Exec Summary

The NRC has determined that nuclear power reactors need additional protection from cyber attacks. The NRC has placed the requirement for these protections on the licensee, not on the vendors. To be successful, we will have to work with our suppliers to insure they deliver products that enable us to comply with NRC regulations.

The purpose of this document is to explain how the new cyber security requirements will affect our dealings with our suppliers and vendors. It will provide some history abut how we got here, then explain what our expectations are for our suppliers and their products. Finally it will include some contract language to support our expectations.

### A Short History of NRC and Cyber Security

The NRC has been concerned about the potential for cyber induced radiological damage for a number of years. After much industry efforts and discussion, the NRC issued 10 CFR 73.54 *Protection of Digital Computer and Communication Systems and Networks*. This regulation specified that licensees had to protect their critical digital assets. In 2011, using NEI 08-09 *Cyber Security Plan for Nuclear Power Reactors* Rev 6, DCPP and most of the rest of the industry submitted a Cyber Security Plan detailing how we would comply with the new requirements.

NEI 08-09 specifies many requirements and controls we are to apply to critical digital assets (CDAs) to protect them from cyber attacks. Controls are actions we take to prevent unauthorized use of the CDA. Controls include such things as passwords, locked cabinets and data-diodes.

### Working with our Vendors

In order to comply with §73.54, we need to procure products from vendors who practice good cyber security and are capable of applying controls to protect the CDA . However, neither the vendors, nor their products have to comply with the NRC regulation. So, if we are to comply with 10 CFR 73.54, we must do one or more of the following:

* Negotiate with our vendors to insure their environment and product are secure…or…
* Develop our own program to insure the products we receive are secure.

In some sense, we will have to do both, more for some vendors, less for others. In order to help our suppliers help us to comply with 73.54, we will share our expectations and, as much as possible, help our vendors meet them.

The major expectations we have when dealing with vendors from a Cyber Security perspective can be grouped into two main areas.

* Expectations for the vendor. This includes the requirement to provide the specified product is free of defects, malware, bugs, and unauthorized components. It also includes that the product is protected while is transit to PG&E.
* Expectations Of the product. We expect the product has the necessary features to enable PG&E to comply with the provisions of NEI 08-09.

## Expectations of the Vendor

These expectations are for vendors that supply equipment or software that will be used on plant systems. These expectations are later turned into requirements during the design and negotiation process. The expectations listed are not exhaustive, nor can they be applied in the same way to all of our vendors. Some vendors/suppliers with require our help to meet these expectations.

Our expectations can be categorized into several areas.

###

### Secure Development and Operating Environment

We expect the vendor to be aware of the cyber threat in the world, and to have established a secure developing and operating environment (SDOE) that provides a high assurance the product(s) they deliver is free of malicious and non-malicious acts. We would like to see such things as the following:

* A written cyber security strategy and how the strategy is implemented.
* Development environment that is isolated from the business environment.
* A Physical Security Plan that provides high assurance DCPP assets are protected while in the Vendor's possession.
* Audit process to insure the vendor's policies are being implemented.
* Documented policies and procedures for patch management and updating their environments. This includes how the vendor protects their environments from third party suppliers.
* Well documented procedure and framework for conduction code reviews.

### Trustworthy Staff

We expect the vendor to have verified the trustworthiness of their people who will work on DCPP assets. We would like to see such things as the following:

* Evidence that the project and environment personnel have passed an investigation that included a credit check and a national and local background check in the last 5 years.
* Cyber Awareness training for their staff.
* An effective behavior observation program to insure personnel remain trustworthy.
* Evidence the programming/manufacturing staff use quality and validation methods to minimize flawed or malformed software and equipment.

### Trustworthy Supply Chain

We expect the vendor to have measures in place that protect the product against supply chain threats and maintain the integrity of software and objects supplied to them. We would like to see such things as the following:

* Evidence of established trusted distribution paths.
* Evidence of validating their suppliers.
* Evidence of how the vendor insures the items they receive have not been tampered with.

### Problem Resolution

We expect the vendor to provide upgrades and patches to their systems/equipment when security issues are identified. We would like to see such things as the following:

* A process to inform DCPP in writing of a flaw with any third party products supplied by the vendor in a timely manner. The vendor will also provide guidance to DCPP about corrective actions, fixes or work-a-rounds, and instruction on monitoring for exploits associated with the flaw.
* A process for users to submit problems and requests for resolution. This process will include how DCPP vulnerabilities are protected from public disclosure.
* A program to discover flaws and exploits associated with the products supplied to DCPP.
* Documentation on how the vendor will maintain DCPP security if the vendor leaves the business.

## Expectations of the Product

To protect the plant from our cyber adversaries, we apply controls to our CDA to prevent them from being used against us. The expectations for products we get center around insuring the product can apply these controls.

For example, one control familiar to all of us is the password. We use a password as a method to prevent unauthorized access, and to insure the person entering the system is an authorized user. In order to use the password control, the product should have the ability to handle a password.

While all CDAs will have controls applied to insure they are protected, not all CDAs will have the same controls applied in the same way. For example, a CDA may not be able to use a password. In such case, we will have to apply an alternate control to protect access to the CDA.

Our expectations can be categorized into several areas.

### System Hardening

We expect the product we receive from the vendor to be hardened against cyber vulnerabilities. Hardening is the process where changes are made to the default configurations of a product to reduce security vulnerabilities. System Hardening includes some of the following:

* A written list detailing all services and ports needed for normal and emergency operation. This list will include the reason the listed services and ports are required.
* All services and users will execute at the least privilege possible.
* All services not needed for operation will be removed.
* All patches and security options are applied at the time of delivery, including any third party software supplied with the DCPP asset.
* Disable all unneeded communication ports, portable media ports, or provide physical barriers.
* Password protect the BIOS.
* If the system uses a heartbeat signal, it will be documented.
* Host intrusion detection will be supplied where possible.

### Access Control

The objective of access control is to provide high assurance only authorized persons or processes can access DCPP CDAs and perform authorized functions. We would like to see the following:

* At a minimum the product will have separate roles for normal operation, maintenance functions and security functions. No guest accounts.
* User rights and permissions for each account will be established at logon. The practice of least privilege will be followed. No user can escalate their privileges.
* Documentation will be provided showing the existence of any vendor configured or manufacturer default accounts, usernames, password, security setting, security codes or any other access methods. Any such access methods or parameters are changed, disabled or removed.
* Any Human Machine Interface (HMI) stations expected to remain logged in continuously will be documented and only permitted to execute operational functions. No maintenance or security functions.
* The product will have a configurable account password management system that supports the PG&E Password Standard.
* No wireless access while in operation.
* User credentials will not be transmitted in the clear.