National Institute for Standards and Technology

Improving Critical Infrastructure Cybersecurity

Executive Order 13636

Preliminary Cybersecurity Framework – XTec Comments

12/13/2013

11180 Sunrise Valley Dr. Suite 310
Reston, VA 20191
Phone: (703) 547-3524
FAX: (703) 547-3533

In response to the NIST Preliminary Cybersecurity Framework, XTec Incorporated would like to submit the comments included in this document. We are interested in being active participants in this new initiative and are certain that our team will have much to contribute. The comments below are our thoughts on the proposed Cybersecurity Framework written with our area of expertise in mind. We are available for additional comment if required and may be reached using the contact information provided in this document.

Regarding the Framework

We understand that the Framework is being created to provide a baseline to all sectors and may be tailored for specific areas. We feel that this initiative should be a source for decision makers and implementers from these sectors to receive Functions, Categories and Subcategories that they find relevant. The five main functions included in the Framework offer enough breadth to be able to encompass various parts of a comprehensive risk assessment but more specific direction will be needed.

For some organizations the Framework may only serve as confirmation of existing risk management practices but many may find the additional guidance new and helpful. We've included some additional areas to consider for sectors that are known to require high security solutions for physical and logical access control. The points below should be considered part of a baseline for the Protect Function. XTec is available to help expand upon the Framework for the sectors for which we are most familiar including government, finance and healthcare.

Function	Category	Subcategory
Protect	Access Control	○ Logical Access to Resources is managed and secured ○ Revocation procedures for credentials ○ Separation between internal and external control systems ○ Administrative level access should be more stringently controlled ○ Supporting an environment of least privilege ○ Securing resources outside the control of the organization ○ Role based access control

The main area for improvement in the framework is that it leaves the risk mitigation process up to the organization and makes it completely voluntary. This makes key aspects of cybersecurity such as authentication and interoperability extremely difficult. Each organization will approach the framework as an exercise in risk tolerance. The expectation that this will lead to any internal process improvement or dedication of resources to the task is uncertain. As governing bodies for this framework become established and efforts arise to turn this Executive Order into common practice, there should be additional means to incentivize participation.

The Framework will yield varying degrees of Tier distribution from organizations. Some will find that their assessment provides minimal gap and therefore little area for improvement. A considerable

number may identify large gaps that will need to be addressed as part of ongoing improvement initiatives. Despite this variance between organizations, a common bar should be set to identify the minimum compliance required to have reasonably mitigated risk for a given sector. There should be a way for organizations to recognize those that have met this minimum in order to provide a basic comfort level for collaboration between these entities, for their customers and any oversight groups including governing bodies.

Another initiative that XTec has been following has been the work of the NCCoE. Their efforts in providing use cases which illustrate sector specific deployments should assist improvement initiatives. Their role should be in line with any NIST Cybersecurity efforts. We believe that their continued collaboration with industry is essential and should be incorporated into forthcoming publications.

The NSTIC initiative is responsible for determining common standards that improve upon current username and password use for identification and authentication. The primary focus of this initiative will be providing improved credentials to the general population since this is their largest pool of participants. Although there may be much to learn from this type of deployment, the systems that comprise Critical Infrastructure (CI) IT and Industrial Control Systems (ICS) should be considered a separate area that will require more stringent security controls and have less risk tolerance. Unfortunately as security improves the focus of criminal organizations will shift to try to bypass these new controls. With the future environment in mind, we should not let any breach, compromised cryptographic algorithm or stolen key in commercial systems potentially impact anything falling under CI Cybersecurity.

There are several publications that have been released in previous years that should help in determining acceptable risk and required levels of assurance. Two notable documents include OMB 0404 and NIST SP-800 63. Due to the critical nature of the systems in question it is our opinion that the electronic identity of the individual needs to be authenticated with an equally strong credential.

The Importance of High Assurance

The Federal Government has provided the foundation for a secure infrastructure that provides personal identity verification with the highest level of assurance for credential holders entering facilities and logging into systems, as directed by a previous Executive Order, Homeland Security Presidential Directive 12. Several years of effort, and a considerable investment, have resulted in the implementation of HSPD-12 and the NIST FIPS 201 Standard. A great deal of knowledge has been gained from implementing these systems and issuing trusted credentials to a large user base. Now is the optimal time to leverage the experience and investment that the Federal Government has made in order to better protect critical infrastructure.

While much of the focus has gone into protecting government agency resources, multiple components of critical infrastructure play an important role in national security and in the daily lives of all Americans. What is deemed as critical infrastructure includes a large part of our transportation systems, power grids, water and gas supply lines, and flood control equipment. Without constant uptime for these services severe disruptive consequences may result. The end goal would be to have practical, effective

and interoperable solutions, that ensure complete control over physical facilities, assets and IT resources that, when combined with proper permissions, equals secure access.

How do you achieve this type of control? Security in cyberspace is suffering from the lack of mechanisms that allow the strong identification and authentication of users. Reliance on User ID and password has become inadequate and susceptible to attacks exposing CI. This has been duly noted under Appendix C of the Framework.

XTec believes that answer lies in long standing credential issuance mechanisms established by the Federal Government under NIST FIPS 201. PIV credentials provide the highest level of assurance (LOA 4), and the ability to electronically authenticate the credential holder in cyberspace. Recently, the federal government issued standards for the PIV-Interoperable credential (PIV-I), the non-government issued equivalent token, and has made available to industry the PKI infrastructure, including the Federal PKI Bridge.

FIPS 201 creates a trust model that starts with the proper vetting of an individual prior to issuance. The issuance process ensures that only appropriate personnel are being provisioned in the systems. Identity source documents, and fingerprint and facial biometrics are collected to aid in determining an identity is valid. Additional safeguards and controls are in place so that abuse at the enrollment level does not occur. Without an active credential, permission assignment and a biometric and/or PIN match, an individual will not gain access into critical systems.

The effort required to properly vet an individual should be paired with equally strong cryptographic hardware. Once identity verification is completed, a smart card based credential is issued and the data is signed by a Federal PKI Bridge authorized Certificate Authority. The Federal Bridge Certification Authority (FBCA) provides the trust anchor for the cryptographic authentication of a credential with a very high degree of assurance. Any less will weaken the authentication and move your assurance level closer to those provided through simple means such as username and password.

Successful authentication is only part of the solution. The pairing of an identity to permissions needs to be sound and allow only enough rights to buildings, assets and systems to fulfill job requirements.

Supporting Least Privilege

Building upon a strong authentication infrastructure, administrative personnel performing maintenance and support activities must have the required authorization and permissions to work operational systems. These permissions must be granted to the user and enables enforcing an environment of least privilege. Roles need to be capable of dividing system capabilities into smaller parts and not provide blanket permissions to resources. This keeps permissions down to the minimum required. Appropriate permissions should not overburden participants and are required to be efficient.

The Importance of Interoperability

Although this guidance is an effort at providing a self-assessment tool for organizations, the ability to work with other entities must be part of a comprehensive risk assessment. Will the credential facilitate access to resources in a disaster recovery scenario?

Deploying solutions that follow federal standards guarantee a quality product and provide the benefit of interoperability. Personnel are going to need to be authenticated for both physical and logical access. There will be times where verification of externally issued credentials will need to take place. A national disaster may, for example, require Emergency Response personnel have immediate access to infrastructure components.

FEMA has been a PIV issuer since 2008. Its employees are capable of identifying themselves with a high degree of certainty since all federal agency credentials have certificates that have been issued under the FBCA. Working with an infrastructure that has been developed with interoperability in mind allows PIV and PIV-I cardholders to be granted access to resources in a disaster scenario with the same degree of confidence as employees. This allows members of the Energy Sector that may not be eligible for a government issued PIV, but require the same level of authentication and authorization, to work as members of this interoperable infrastructure. Interoperability is not limited to just the smart card but also incorporates flexibility in credential form factors, including mobile devices.

The Ability to Work with Mobile

The highest level of assurance may not be needed at all times when verifying the identity of an individual. There are areas that offer less risk and a means of authentication at a slightly lower level of assurance may be acceptable. For this scenario we suggest the use of derived certificates, and the flexibility that they offer to those that are already PIV or PIV-I card holders.

A derived certificate has a direct relationship to, and is generated from, the certificates stored on the PIV or PIV-I card. These derived certificates may then be downloaded onto a mobile device which could then be used in the authentication process instead of the smart card: the user will authenticate themselves with the mobile device that they normally carry. Near field communication facilitates the authentication process between the mobile device and the contactless reader. The same interface may be applied for both physical and logical access.

XTec Past Experience with Critical Infrastructure

Since the implementation of HSPD 12, XTec has been an industry leader in providing Identity Management and Credentialing systems to federal government agencies including DHS, DOS, DOL, DOJ and many others. Additionally, XTec, in partnership with Entrust, is also certified to issue PIV-Interoperable credentials (PIV-I) to commercial customers.

All of our systems are engineered solutions with maximum security as the objective. We have received numerous successful Certification & Accreditation assessments both under the DoD Information Assurance Certification and Accreditation Process (DIACAP) and the National Assurance Certification and Accreditation Process (NIACAP). In addition, XTec is currently pursuing FedRAMP certification for our cloud-based systems.

XTec leads the industry in deploying LOA 4 end-to-end physical access control solutions for Federal Agencies that must comply with HSPD-12, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116, FIPS 201, and FICAM guidance. The XTec physical access control solution includes GSA approved smart card readers, XNodes, supporting network infrastructure and

management interfaces all engineered to ensure that physical threats are isolated from the secured facilities.

XTec's vast experience in physical access control, logical access control and the issuance of secured credentials is available to NIST. We are willing to assist in the fulfillment of this Executive Order. As a firm believer in the value of protecting critical infrastructure, XTec is available for comment and is willing to offer insight that pertains to our areas of expertise which we believe will be valuable in the creation of a Cybersecurity Framework.

Points of Contact

Albert Fernandez
President
af@xtec.com
(305)357-8833

Tony Arner
Controller
aarner@xtec.com
(305)357-8813

Danny Vital
Senior Engineer
dvital@xtec.com
(305)357-8821