Comments of the California Public Utilities Commission

Response to the National Institute of Standards and Technology,
U.S. Department of Commerce,
"Improving Critical Infrastructure Cybersecurity Executive
Order 13636:
Preliminary Cybersecurity Framework"

December 13, 2013

Introduction

The California Public Utilities Commission (CPUC) hereby submits comments to the National Institute of Standards and Technology's (NIST) "Preliminary Cybersecurity Framework (Framework),"[1] developed pursuant to Executive Order 13636 (EO).[2] The EO was issued on February 10, 2013, and directed NIST to convene a process to develop a Cybersecurity Framework that can be applied to the 16 critical infrastructure sectors, as identified by the United States Department of Homeland Security (DHS).[3] The CPUC has a vested interest in the outcome of this effort as we, as well as the other state utility commissions, are the entities responsible for ensuring the cybersecurity of the utilities under our jurisdiction, which may include water, electric, natural gas, and communications utilities that serve the distribution, retail, and/or local needs of the residents of California.[4]

Since NIST issued the Preliminary Cybersecurity Framework was published in the Federal Register, NIST has held five workshops over the past year in preparation for the release of this document, the most recent being in November in Raleigh, North Carolina.[5] The EO directed NIST to finalize the Framework within one year of the release of the EO- February 10, 2014

The CPUC, and other state commissions, are addressing the multitude of cybersecurity issues faced by our utilities under our jurisdiction and are in various stages of outreach and interaction with them regarding cybersecurity. CPUC Staff has participated in prior activities at NIST in the development of the NISTIR 7628, and has previously submitted comments to NIST about the role of states regarding cybersecurity. Additionally, the CPUC is statutorily tasked with ensuring that utility

[1] *Request for Comments on the Preliminary Cybersecurity Framework*, 78 Fed. Reg. 64478, issued on October 29, 2013, available at http://www.gpo.gov/fdsys/pkg/FR-2013-10-29/pdf/2013-25566.pdf.

[2] Exec. Order 13636, 78 Fed. Reg. 11737, issued on February 19, 2013, available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[3] The full list of critical infrastructure sectors can be found on the DHS web site at http://www.dhs.gov/critical-infrastructure-sectors (last accessed November 25, 2013).

[4] These comments also reflect the input from staff at a number of other state utility commissions.

[5] CPUC Staff attended the workshops in San Diego, CA and Dallas, TX.

investments, notably in the electricity sector, include "cost-effective full cyber security."[6] The CPUC has also required that future investments in the Smart Grid by our electric utilities include a cybersecurity strategy,[7] and CPUC Staff have authored a White Paper addressing the role and possible steps that the CPUC may take in the future regarding our role in ensuring the cybersecurity of utility investments.[8] The CPUC looks forward to continued collaboration with NIST in the development and finalization of this Framework to support efforts to address cybersecurity risks.

Preliminary Cybersecurity Framework

This Framework is designed by NIST to complement an organization's existing cybersecurity practices. Should an organization not have any cybersecurity practices, this document can help inform it to develop one through practical steps and processes. The Framework makes use of and references existing standards and best practices.

It is important to note that the Framework is not a standard, nor is it a mandate. It is based on a risk-management approach to cybersecurity, similar to the guidance documents issued by the Department of Energy last year around risk-based approaches to cybersecurity for electric utilities.[9] As such, the Framework is centered on five

[6] Cal. Pub. Utils. Code, Sec. 8360, subd. (b).

[7] D.10-06-047, *Decision Adopting Requirements for Smart Grid Deployment Plans Pursuant to Senate Bill 17 (Padilla), Chapter 327, Statutes of 2009*, issued on available at http://docs.cpuc.ca.gov/PublishedDocs/PUBLISHED/FINAL_DECISION/119902.htm.

[8] "*Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission*", issued on September 19, 2012, available at http://www.cpuc.ca.gov/NR/rdonlyres/D77BA276-E88A-4C82-AFD2-FC3D3C76A9FC/0/TheEvolvingRoleofStateRegulationinCybersecurity9252012FINAL.pdf; *See also*, "Cybersecurity for State Regulators", issued on February 2013 by the National Association of Regulatory Utility Commissioners available at http://www.naruc.org/Grants/Documents/NARUC%20Cybersecurity%20Primer%202.0.pdf.

[9] *See* "Electricity Subsector- Cybersecurity Capability Maturity Model", issued on May 31, 2012 by the Department of Energy, available at http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20%28ES-C2M2%29%20-%20May%202012.pdf; and "Electricity Subsector- Cybersecurity Risk Management Process," Department of Energy (May 2012) avail able at http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf.

Functions: Identify, Protect, Detect, Respond, and Recover. These functions provide a high-level strategic view of an organization's management of cybersecurity risk. Inside each Function includes a corresponding set of Categories, Sub-Categories, and Informative References to help guide implementation of the Function. The Framework also includes a section on protecting privacy and civil liberties in the application of the Functions' Categories and Sub-Categories.

Next, the Framework contains a "Profile" which can act as a roadmap for implementation and outcomes. This Profile can align implementation with industry standards and best practices, as well as identify areas for improvement by comparing a "current" profile with a "target" profile. This can then help with an organization to prioritize needs across the organization to meet the target profile.

Finally, the Framework provides a set of "Tiers" by which an organization can describe how cybersecurity is managed across the organization. The Tiers help define the current risk management practices against a set of characteristics and maturity. The Framework defines Tiers as ranging from 1 ("Partial") to 4 ("Adaptive"), which can also reflect any informal implementations to more formal implementations or a risk-informed approach.

Comments on the Framework

NIST asks for comments on the Framework on a number of topics relating to implementation. While not necessarily in the order sought by NIST, the comments below touch on most of the questions asked by NIST.

Since this Framework is targeted at several critical infrastructure sectors that are under the jurisdiction of state utility commissions, it is important that this process reflect state commissions will also have a role in implementing this Framework by potentially granting cost recovery for implementation, as well as using this Framework to guide any monitors of how a utility implements a cybersecurity strategy or program. As noted above, the CPUC is the entity responsible for overseeing utility infrastructure investments and ensuring that the utilities have appropriate and cost-effective cybersecurity strategies and protocols in place.

Additionally, the CPUC is interested in ensuring that as a utility uses this Framework that it is consistent with the goals of California and supports the cybersecurity of their operations and services. Indeed, as the agency directed to ensure reliability of crucial resources such as electricity, natural gas, and water services, the

CPUC needs to have some level of assurance that this Framework will adequately provide for a process to ensure the cybersecurity of these sectors. For example, California Public Utilities Code Section 8360 makes it the policy of the State of California to modernize the electric grid, but also much contains "cost-effective full cyber-security." In order to accomplish this policy, the CPUC is directed to "adopt standards and protocols to ensure functionality and interoperability" including standards developed by NIST.[10]

Finally, the CPUC fully supports and recognizes the tremendous effort undertaken by NIST. The CPUC supports the development and finalization of a cybersecurity Framework as a means to develop a structure by which a company can use to determine best next steps regarding their cybersecurity practices. We certainly recognize that this effort required significant work by the team at NIST, and congratulate them on the work accomplished so far.

Specific Comments on the Framework

1) The five Functions continue to omit an on-going "learning" function. The description of the Functions, and associated Categories and Sub-Categories, do not provide a clear and on-going process where each step can learn from other Functions. For example, as the processes are developed in the "Identify" Function and implemented in the "Protect" Function, there is no clear linkage between the Functions for learning or proof in the implementation of the Protect Function. Not having an on-going learning process between all 5 Functions may limit the ability of the Framework to be useful and/or successful across a company.

1.a) The Framework seems to only mention information sharing in passing; once in describing what a "Tier 4 – Adaptive" entity should be doing, and in the Framework Core under Identify – Risk Assessment – ID.RA.2. The Framework may be improved by more often integrating and emphasizing communication methodologies and platforms to share information.

The 5 Functions of the Framework Core seem to lack an emphasis of implementing plans and communications (both internally and with and between external stakeholders), and how to improve and use lessons learned after simulated and real attacks. Perhaps a "Learning and Sharing" Core Function

[10] Cal. Pub.Utils. Code, Sec. 8362, subd. (a).

could be added to tie together the other Functions, as well as to open the Functionality from a singular entity effort to an industry-supported process.

The Framework has no mention of best practice for awareness, assessment, and possible integration of emerging cybersecurity technologies; i.e. learning about unidirectional gateways as an alternative to firewalls, assessing application into operations, and if chosen – implementation of technology integration. This could be tied into a "Learning and Sharing" function.

2) The Framework seems very outcome driven, as opposed to having a living process to drive ongoing development of cybersecurity tools. For example, the Preliminary Framework describes the categories in terms of "outcomes," rather than as a more on-going process. Indeed, many of the categories identified under the Functions describe actions in response to an event, instead of describing an on-going set of protocols or processes that can be linked to other Functions or future actions.

3) There is no clear identification of responsibility or roles across an organization. There are assumptions made in the Category and Sub-Categories of the identification of "personnel" to take some actions, but there is no specific identification of types of personnel responsible for certain actions. For example, in the "Identify" Function, there is a category called "Asset Management" which includes identification of personnel, but in the "Detect" Function, there is a category called "Security Continuous Monitoring" where no individual or personnel roles are identified.

3.a) It's not clear to what extent the Framework addresses security personnel planning and management. The Core Function, Identify – Asset Management, ID-AM.6 simply states: "Workforce roles and responsibilities for business functions, including cybersecurity, are established." Do the referenced standards include best practices available to suggest what position types enable cybersecurity development and management, and what corporate structures can be considered for these staff? (i.e. who the CISO and CIO report to, and how these positions make and carryout decisions with operations, corporate, and executive staff). In addition, there is a lack of substantial discussion of practices listed to create and sustain a culture of security among staff at an entity responsible for protecting critical infrastructure (culture to protect PII is mentioned though in Appendix B: Methodology to Protect Privacy and Civil Liberties for a Cybersecurity Program).

4 While the Framework states that it allows for flexibility in implementation, the document would be better served by specifically describing how it is flexible, both in its implementation as well as how it can be adapted across multiple sectors. In previous NIST workshops, participants have expressed clear preferences that the Framework be allowed to fit the varying needs of the various sectors.

Additionally, the Framework focuses on the generic process of what to do, but does not address implementation of the process. Appendix A, for example, lists steps such as "Organizational information security policy is established" and "Physical access to resources is managed and secured" but provides no information on how to achieve these steps, or verify their achievement.[11] Similarly, the focus on generic process leaves out essential items such as the need for independent security audits and utilization of security compliance monitoring tools. The usefulness of the Framework would be enhanced by providing specifics on how discrete process items can be implemented and verified, such as through references to specific examples, case studies, models and real-life scenarios.

One of the key attributes identified in the EO is that the Framework is to be cost-effective to implement. If it is NIST's intention that the Framework is to be flexible, then NIST should also identify a set of minimum actions to encourage flexibility as well as tools for cost-effective implementation of the Framework.

6) The CPUC supports the use of the Framework Implementation Tiers proposal in the Framework. The Tiers are designed to allow an organization to measure the maturity of its risk-management process. In the workshops, many organizations and individuals representing various sectors objected to the use of Tiers due to the potential use of the Tiers by regulators, and voiced that NIST does not do an adequate job of explaining the purpose of the Tiers. The CPUC suggests adding a Tier 0 indicating where nothing has taken place, while taken alone may reflect poorly upon an organization, but still provides a baseline for risk management maturity. The Framework tiered design is a positive approach to developing general policies

[11] For example, one of the more common entry points for cyber intrusions results from the failure to consider security in customer Internet application development. To address this, the wording in PR.IP-2 should be changed to "A System Security Development Life Cycle" to help ensure that security is an upfront consideration in application development.

addressing cybersecurity threats. However, the migration steps between tiered levels are not explicit in the Framework. Metrics for determining the status of an organization, including third-party auditing, are important aspects of a tiered system. Additionally, metrics would allow for a more fluid framework that emulates the constantly evolving technologies and threats in cybersecurity.

State utility commissions can play a role in setting benchmarks and baselines in the implementation of the Framework to continue driving progress on the document, sharing information with others, and identifying new needs or actions for future versions of the Framework.

8) NIST needs to provide more clarity regarding the on-going governance of the Framework, especially concerning contemplated revisions or management of the Framework. Without a clear vision of who is responsible for the management of the Framework, it risks becoming stale quickly and as a practical result being potentially set aside by the industry.

9) It remains unclear how NIST expects the privacy and civil liberties methodology to be fully integrated with the rest of the Framework. We laud NIST for being proactive on the topic, but it deserves more prominence to reduce the likelihood that it is perceived as merely an after-thought. For example, in the "Identify" Function and "Asset Management" Category, there is no identification of who is responsible for identifying the Privacy categories and sub-categories. The Privacy "Asset Management" Category simply states that an organization should identify the PII of people potentially impacted by an event, not who should be doing the cataloging. Also absent is an on-going "learning" ability or an indication that actions should be cross-functional.

10) The Framework's position as a part of an organization's cybersecurity policies needs to be clearer. The needs are different for organizations with mature cybersecurity capabilities versus those needing improvement. However, the Framework seems to present a one-size-fits-all approach that does not quite fit various levels of maturity. While such a structure is useful from a project management standpoint, the effectiveness of this model as a tool by cybersecurity professionals, regardless of industry, is not clear. The Framework lacks actionable items and how to incorporate them into an overall cybersecurity policy. Clarity on the relationship between the Framework and overarching policy models, such as the Electricity Subsector Cybersecurity Capability Maturity Model, would provide decision makers with a more complete picture for building and maintaining individualized, complete, and secure

cybersecurity policies. Additionally, explicit policies should be included in the framework regarding such things as continuity of operations, protection of privacy and civil liberties, and strategic recovery of assets.

Use and Role of Standards and Best Practices

11) The Framework should include an upfront, basic list of fundamental controls and common sense security best practices designed to address historical control weaknesses associated with recurring cybersecurity intrusions. The standards and best practices referenced by the Framework are essential, but in isolation have not been effective in the past. Organizations often find it challenging, if not impossible, to determine which controls and practices are critical and relevant to addressing known and otherwise easily addressable security threats. A solution to this problem would be the development of a companion authoritative master list that describes the control weaknesses (and corresponding best practices) that have historically enabled successful cyber intrusions in critical control infrastructure systems, including least privileged access, authentication, anti-malware, compliance management, application development, back door accounts, defense in depth and unsecured Wi-Fi. This could be developed by a synergistic combination of the activities and outputs of Sections 4 and 7 of Executive Order 13636. The Attorney General, the Secretary of Homeland Security and the Director of National Intelligence could provide NIST and the critical infrastructure industry an authoritative master list generically describing the control weaknesses. Making these control weaknesses an outcome objective of the Framework could help provide reasonable assurance that at least these negligent control weaknesses are not repeated.

12) The Framework makes an excellent start at addressing a major problem of implementing a security framework: the difficulty in identifying what standards exist and which are most important. The Framework would provide greater benefit by providing a master list that cross-references existing best practices and standards that can be easily referenced.[12]

13) The Framework would profit from a greater level of specificity with respect to critical infrastructure. Executive Order 13636 called for a focus on the identification of

[12] CPUC would like to note that NIST should consider that references to ISO-IEC 27001 should be verified and updated. This standard was updated in October 2013, and several references to it in the Framework may no longer be applicable.

cross-sector security standards applicable to critical infrastructure. While there is a reference to ANSI/ISA 99.02.01 pertaining to Industrial Automation and Control Systems, the Framework would benefit from more references to standards and best practices specifically applicable to critical infrastructure, SCADA or industrial control systems.

Missing topics

14) One topic that is not addressed as part of the Framework is adoption. An on-going concern by all parties involved in this effort, including the Administration, is the use of this Framework which has been characterized as voluntary. In order to encourage the use of the Framework, the Department of Homeland Security (DHS) has proposed the use of several types of "incentives" to be given to organizations to adopt and use the Framework. More explanation should be given by NIST, DHS, or the Adminstration regarding how the Framework will interact with any DHS incentive. The CPUC is interested in this effort as one of the incentives identified by DHS is to pay for or help offset the cost of implementation of the Framework. For example, if an organization indicates that it will cost $1 million to implement the Framework, DHS may offer funds to pay for half of it. This could be problematic for state utility commissions because state utility commissions are responsible for determining if any remaining costs to a utility are reasonable. The CPUC has a well-defined obligation and a substantial interest in being part of this effort to ensure that the Framework provides adequate means to ensure robust cybersecurity practices, and be mindful of costs because it is likely that our regulated utilities will eventually seek rate recovery for implementing the Framework.

15) The Framework does not sufficiently discuss cybersecurity-specific mitigation strategies and lacks applicability to physical cybersecurity infrastructure in the various industries. The Framework includes some categorical information which is more specific and Appendix C also contains areas where improvement of standards can be focused. While these lists are explicitly stated as being non-exhaustive, it would be useful if the framework presented ideas or strategies for developing the actual mitigation efforts that may be used to address cybersecurity concerns. For instance, the framework could reference ICS-CERT Recommended Practices[13] or the Australian

[13] "Recommended Practices, Industrial Control Systems Cyber Emergency Response Team," available at ics-cert.us-cert.gov/Introduction-Recommended-Practices.

Signals Directorate "Strategies to Mitigate Targeted Cyber Intrusions."[14] This and additional information could be combined to produce descriptive processes that identify specific risks and mitigation strategies inside of the Framework.

16) The Framework lacks a set of metrics by which a company can identify success. Additionally, there appears to a lack of identification or reference to best practices that a company could follow. It is unclear whether any of the referenced standards contain associated metrics as the standards in Appendix A provide no description of the standards. In order to help determine appropriate metrics or identification of best practices, it may be useful for NIST to support an initial testing phase of the Framework prior to a wider push for adoption of the Framework across the critical infrastructure sectors.

Conclusion

The CPUC continues to support the development of a voluntary cybersecurity framework as envisioned in the EO. The CPUC will continue to work with NIST, and other relevant agencies and entities to craft a framework that can be used by our regulated utilities in a way that is constructive and encourages managing cybersecurity risk. The CPUC offers to NIST any assistance we may be able to provide in finalizing the Framework in a manner that helps foster more robust cybersecurity practices and implementations. We thank NIST for the opportunity to provide comments on this document.

Respectfully Submitted,

/Christopher Villarreal/

Christopher Villarreal, Senior Regulatory Analyst
Elizabeth Dorman, Principal Legal Counsel
for the
Public Utilities Commission of the State of California

[14] "*Strategies to Mitigate Targeted Cyber Intrusions*," Australian Signals Directorate, October 2012, available at www.asd.gov.au/infosec/top35mitigationstrategies.