CONTEXT FOR THE REVIEW OF CYBER SECURITY PLANS

Under section 715 of the Executive Law, the Office of Cyber Security (OCS) is "dedicated to the protection of the state's cyber security infrastructure, including, but not limited to, the identification and mitigation of vulnerabilities, deterring and responding to cyber events, and promoting cyber security awareness within the state" and for "statewide policies, standards, programs, and services relating to cyber security."

The State has received a request from the Nuclear Regulatory Commission (NRC) for comments on cyber security plans submitted by licensees of four nuclear power plants in New York State. This request arises in the context of proposed amendments to the operating licenses for these plants.

The regulatory framework applicable to nuclear power plant licensees requires that the physical protection programs of those licensees "provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks" (10 CFR 73.54[a]). To this end, the regulation requires licensees to establish, implement, and maintain a cyber security program for the protection of digital computer and communication systems and networks (10 CFR 73.54[b][1],[2]). Licensees are further required to "establish, implement, and maintain a cyber security plan that implements the cyber security program" (10 CFR 73.54[e]; see also 10 CFR 73.55[b][8]). The cyber security plan must:

- describe how the requirements of 10 CFR 73.54 will be implemented;
- account for the site-specific conditions that affect implementation;
- include measures for incident response and recovery for cyber attacks, including how the licensee:
    - maintain the capability for timely detection and response to cyber attacks;
    - mitigate the consequences of cyber attacks;
    - correct exploited vulnerabilities; and
    - restore affected systems, networks, and/or equipment affected by cyber attacks.

  (10 CFR 73.54[e][1],[2]).

To assist licensees in complying with the requirements of 10 CFR 73.54, the NRC issued a Regulatory Guide entitled "Cyber Security Programs for Nuclear Facilities" (Regulatory Guide 5.71, January 2010). The Regulatory Guide (RG) outlines the process for identifying those Critical Digital Assets (CDAs) that must be protected from cyber attack and specifies the 17 required elements of a cyber security plan that satisfies the regulation. A template for a generic cyber security plan which licensees may use to comply with the licensing requirements of 10 CFR 73.54 is also included as an appendix to the RG.

Licensees are not required to use the template provided in the RG. In this regard, we note that the Nuclear Energy Institute (NEI), a group representing licensees, has developed its own guidance, which is embodied in NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors." Both the RG and NEI 08-09 rely on controls identified in National Institute of Standards and Technology (NIST) standard 800-53, "Recommended Security Controls for Federal Information Systems." The cyber security plans that are subject to this review are all based on NEI 08-09.

The RG also includes extensive guidance on the development of a compliant cyber security program including details on identifying digital assets as CDAs, addressing potential cyber security risks to CDAs, implementing defensive strategies to protect safety, security, and emergency preparedness (SSEP) functions, identifying security controls to address the potential cyber risks to a CDA, and guidance associated with the policies and procedures relating to the implementation of the cyber security program.

Under the provisions of 10 CFR 50.4 and 50.90, implementation of the cyber security plans and any revisions thereof are considered amendments to the physical security plans that are incorporated into the facilities' operating licenses and are, therefore, subject to the review and approval of the NRC. In each of the instances that are under review by OCS, the NRC has already made a proposed determination that the amendment of the license presents no significant hazard consideration (see, 75 FR 62596, 75 FR 51492, 75 FR 62594). Under 10 CFR 50.92, this determination means that the NRC found that the operation of the facility in accordance with the proposed amendment would not: (1) involve a significant increase in the probability or consequences of an accident previously evaluated; or (2) create the possibility of a new or different

kind of accident from any accident previously evaluated; or (3) involve a significant reduction in a margin of safety.

GENERAL COMMENTS ON THE REVIEW OF THE CYBER SECURITY PLANS

In establishing the context and scope for the review of the cyber security plans, it is important to note the distinction made in the regulation and the RG between the "cyber security plan" and the "cyber security program." Under the RG, the "cyber security plan" is a high-level, policy document that describes how the licensee will implement the requirements of 10 CFR 73.54 at a nuclear facility. In contrast, the "cyber security program" encompasses site-specific analysis of digital computer and communication systems and networks, defense-in-depth protective strategies, security controls, continuity of operation policy, training and awareness, policies and procedures to implement the cyber security program. Most notably, licensees are not required to submit policies, implementing procedures, site-specific analyses, or other supporting technical information to the NRC for prior review and approval. Such information need only be made available for inspection by the NRC staff.

Given the foregoing, the documents reviewed by OCS encompass only the cyber security plans submitted by the licensees, including the proposed implementation schedules for portions of the plans, and the licensees' responses to requests for additional information from the NRC. No information concerning the digital computer and communication systems and networks of the licensees or the actual controls, configurations, and procedures implemented by the licensees has been reviewed.

In preparing to undertake the review of the cyber security plans, OCS consulted with both the NRC and the New York State Energy Research and Development Authority (NYSERDA). Bhalchandra K. Vaidya, Licensing Project Manager with the NRC indicated that New York should evaluate the three components of the NRC's proposed determination of no significant hazard consideration and whether New York would require anything in addition to what is already required by the NRC. In addition, OCS discussed the potential scope of its comments with Alyce Peterson, the State Liaison Officer Designee at NYSERDA, who expressed the opinion that OCS was not constrained in what aspects of the plans might be subject to comment.

OCS has no existing cyber security requirements applicable to industrial facilities such as nuclear power plants and our Statewide Information Security Policy, applicable to State agencies, is a generic document similar to the NRC's policy template. In light of the foregoing, OCS has undertaken the following:

- Review of the cyber security plans, implementation schedules, and licensee's responses to requests for additional information from the NRC.
- Comparison of the cyber security plans to the New York State Information Security Policy (PS03-002) and Information Classification and Control Policy and Standard (PS08-001).

COMPARISION TO STATEWIDE POLICIES AND STANDARDS

Under New York's Information Classification and Control Policy and Standard (PS08-001), each information asset must be classified using three principles (confidentiality, integrity, and availability) and, based on this classification, certain controls must be implemented to secure the information asset. OCS has compared the NRC and NEI guidance (regulations, RG, and NEI 08-09) to the controls identified in PS08-001. Unless a specific reference is provided, this guidance will be referred to as "Guidance."

For purposes of our review, it was assumed that all CDAs identified by the licensees would be classified with high confidentiality, integrity and availability ratings under PS08-001. For assets with this classification, the following are the controls that would be implemented under PS08-001 that cannot be readily identified in the documents provided or are weaker than those that would be implemented under New York's policy and standard:

- PS08-001 Controls No. 1 and No. 47 require that agencies review all security procedures and controls, including the access control policy and procedures, at least annually to ensure their effectiveness in the face of changing threats. 10 CFR 73.55(m) requires a review only every 24 months.

- PS08-001 Control No. 6 requires agencies to ensure that more than one person has access to the CDA to ensure business continuity. This control could not be readily

identified in the Guidance, but may be part of the contingency plans that are part of the licensees' detailed cyber security programs.

- PS08-001 Control No. 9 requires that electronic storage media and devices be issued, owned, controlled or approved by the agency. This includes media used to record and store data, but not limited to tapes, hard drives, USB flash drives, memory cards/chips, CDs, and diskettes. This requirement is not specifically laid out in the media protection processes found in the Guidance.

- PS08-001 Control No. 10 requires that agencies ensure the security of alternate storage sites. The Guidance does not clearly provide for the review and approval of physical/cyber controls at alternate storage sites.

- PS08-001 Control No. 56 requires that executive management designate the level of management who can give written approval for transportation or storage of information outside of an approved storage facility and for transmission of information outside the agency. All such approvals must be documented by designated management. The Guidance does not appear to require management review and/or approval of external systems used for storage/transmission. While this control could not be readily identified in the Guidance, it may be part of the licensees' detailed cyber security programs.

- PS08-001 Control No. 13 requires the creation and implementation of written procedures to keep track of individual documents, files, devices or media which contain sensitive data and the individuals who have possession of them. This control could not be readily identified in the Guidance, but may be part of the licensees' detailed cyber security programs.

- PS08-001 Control No. 21 requires information custodians to monitor environmental protection measures (e.g., HVAC, fire suppression) for problems and correct as needed. While the Guidance includes implementation of environmental protection security controls (e.g., temperature, humidity), there is no mention of monitoring those controls to ensure they are functioning properly.

- The Guidance indicates that the length, strength, and complexity of passwords balance security and operational ease of access within the capabilities of the CDA. Given that these are CDAs, a minimum length should be specified. Under New York's Cyber Security Standard S10-004, User Password Management, the password length minimum is 8 characters.

ADDITIONAL GENERAL OBSERVATIONS ON THE GUIDANCE AND THE PLANS

- Under the Guidance, the cyber security plans and the cyber security programs focus on CDAs and systems, structures, and components (SSCs) in the balance of plant (BOP) that could directly or indirectly affect reactivity at a nuclear power plant, resulting in an unplanned reactor shutdown or transient. While licensees have added a reference to SSCs in the Scope and Purposes sections of the plans, controls in the cyber security plans refer specifically to CDAs. To avoid confusion, the cyber security plans should be clarified to indicate that the controls apply to both CDAs and SSCs.

- In many instances, cyber attacks come from unexpected sources. For example, the initial attack vector for Stuxnet worm may not have been directly focused on a CDA or SSC. Analysis indicates that the worm may have been introduced into the networks of the target by infecting an employee or third party, such as a contractor with access to those networks and may have been introduced by removable drive, the worm then searching out those computers that do communicate with industrial control systems (see, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf).

  Given the sophistication of the attacks occurring in the current environment and the criticality of the systems within these facilities, it is our view that the cyber security plans should be clarified to encompass all digital assets within the facilities, not just critical systems, to ensure the licensees address as many potential pathways for attack as possible.

- Portions of the Guidance appear to limit the obligation to provide awareness training to "appropriate facility personnel, including contractors." In light of the pervasiveness of the

threats and the interconnectedness of networks, discussed above, such training should be provided to all employees and contractors.

- Cyber security plans should include the protection of information assets that can be used in a cyber attack. Information security controls should be applied to these information assets regardless of form or format. For example, paper documents containing blueprints for the plant should have confidentiality, availability and integrity controls applied. It is possible that these controls are included in the licensees' physical protection programs and were, consequently, outside the scope of this review.

- None of the licensees submitted implementation schedules that include completion dates for the key intermediate milestones identified by the NRC other than the latest date, December 31, 2012, permitted by the NRC. Full implementation of cyber security plans will not occur until significantly later, one licensee identifying February 26, 2016, as its deadline for full implementation.

  While it is clear that the implementation of cyber security plans and programs at the facilities in question represents a large and complex undertaking, implementation schedules that identify the latest possible dates for the completion of all milestones is not indicative of a rational approach to project management. Establishing an implementation schedule that includes reasonable risk, effort, and resource based dates for the completion of individual key intermediate milestones would appear to be essential to managing such an undertaking.

  It appears that at least one of the licensees had submitted an implementation plan that identified sequential completion of various intermediate milestones, but replaced that plan when NRC agreed to a modification of the template for the cyber security plan implementation schedule. It appears, from the letter from NRC to the NEI dated March 1, 2011, that NRC expected the licensees to submit site specific schedules:

  > The NRC staff understands that the template was written generically, and licensees that use the template to develop their proposed implementation schedules may need to make changes to ensure the submitted schedule

accurately accounts for site-specific activities. As site specific schedules are developed, it is important to note that in addition to the full program implementation date outlined in the schedule, the milestones that need to be accomplished by December 31, 2012 are of particular importance to the NRC.

Further, while we are, as noted above, cognizant of the magnitude of the undertaking, it is our view that full implementation of the cyber security plans should be completed sooner than the dates identified in the current implementation schedules. These dates, which are three to four years in the future, do not appropriately reflect the gravity of the cyber security risks that confront these critical facilities.

- The licensees and the NRC have found that the operation of the facility in accordance with the proposed amendment would not: (1) involve a significant increase in the probability or consequences of an accident previously evaluated; or (2) create the possibility of a new or different kind of accident from any accident previously evaluated; or (3) involve a significant reduction in a margin of safety.

  In defending this assumption, the Constellation Energy Nuclear Group (R.E.Ginna Nuclear Power Plant/Nine Mile Point Nuclear Station) states that the plan "does not require any plant modifications, alter the plant configuration, require new plant equipment to be installed, alter accident analysis assumptions, add any initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected. The plan establishes how to achieve high assurance that nuclear power plant digital computer and communication systems and networks associated with certain systems and functions are adequately protected against cyber attacks. This protective function has no impact on the probability or consequences of an accident previously evaluated."

  Entergy Nuclear Operations, Inc. (James A. Fitzpatrick Nuclear Power Plant/Indian Point Nuclear Power Plant) states the plan "does not alter accident analysis assumptions, add any initiators, or affect the function of plant systems or the manner in which systems are operated, maintained, modified, tested, or inspected…does not require any plant

modifications which affect the performance capability of the, structures, systems, and components relied upon to mitigate the consequences of postulated accidents.

However, in their implementation schedules, all licensees state that "[i]solating the plant systems from the internet, as well as from the corporate business systems is an important milestone in defending against external threats. While the deployment of the barriers is critical to protection from external cyber threats, it also prevents remote access to core monitoring and plant data systems for reactor engineers, plant operations, and other plant staff. This elimination of remote access to reactor core monitoring systems may require the development and execution of a detailed change management plan to ensure continued safe operation of the plants."

There appears to be inconsistency in these statements. Without a full understanding of the nature of the changes required, it is impossible for us to comment on whether or not this could represent a significant hazard.

RECOMMENDATIONS

Given the critical nature of the facilities in question and evidence of the real and growing cyber threats against these types of facilities (e.g., Stuxnet, NightDragon), it is imperative that cyber security be made a priority. While the creation of cyber security plans is an important first step, programs need to be in place to ensure that these plans are being implemented at an appropriate pace and, once implemented, are being followed. In addition, it is also important for the licensees to provide transparency into their efforts to mitigate cyber security vulnerabilities while they are progressing toward full implementation of the required cyber security plans Finally, OCS recommends that the implementation of the cyber security plans be substantiated by NRC inspections.

SPECIFIC CYBER SECURITY PLANS

Constellation Generation Group, LLC – Nine Mile Point Nuclear Station Units 1 and 2 and

R. E. Ginna Nuclear Power Plant

Full implementation of the cyber security plans by February 26, 2016. [See general comment on implementation schedules, above.]

Entergy Nuclear Operations, Inc. – James A. Fitzpatrick Nuclear Power Plant

Full implementation of the cyber security plan by December 15, 2014. [See general comment on implementation schedules, above.]

Entergy Nuclear Operations, Inc. -- Indian Point Generation Station Units 1, 2, and 3

Full implementation of the cyber security plan by December 15, 2014. [See general comment on implementation schedules, above.]