Current Risk Management Practices

The National Institute of Standards and Technology (NIST) solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

1. ***What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?***

Three challenges in improving cybersecurity practices across critical infrastructure include (1) the tailoring of guidance to fit the needs of an organization or industry; (2) development of cybersecurity programs that effectively manage risks to critical systems; and (3) workforce development initiatives to ensure organizations and industries within the nuclear sector have access to highly skilled, trained, and qualified staff and support personnel.

Tailoring of Guidance (Challenge 1)

In March 2009, the U.S. Nuclear Regulatory Commission (NRC) issued a cyber security regulation at Title 10 of the *Code of Federal Regulations* (10 CFR) 73.54, "Protection of Digital Computer and Communications Systems and Networks" that applies to existing operating power reactor licensees and combined license applicants. 10 CFR 73.54 required operating power reactor licensees to submit a cyber security plan and an implementation schedule to the NRC for review and approval; all operating reactor licensees met this significant milestone. Combined license applicants submit their cyber security plans on a site specific schedule. The plan must show how the facility identified (or would identify) critical digital assets and describe its protective strategy, among other requirements.

In January 2010, the NRC published comprehensive guidance to licensees and combined license applicants on an acceptable way to meet the requirements of 10 CFR 73.54 (http://nrc-stp.ornl.gov/slo/regguide571.pdf). This guidance is titled *Regulatory Guide* (RG) 5.71, "Cyber Security Programs for Nuclear Facilities." The guidance includes recommended best practices from such organizations as the International Society of Automation, the Institute of Electrical and Electronics Engineers, and the NIST, as well as guidance from the Department of Homeland Security. NRC staff utilized NIST Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems," Revision 3 to inform the regulatory guidance development. The unique requirements of commercial nuclear power plants, extent of regulations governing critical functions performed by digital technologies in use at these plants, and the contributions of experts across multiple fields and programs were factors heavily influencing how the NRC dispositioned the high baseline security controls contained in NIST SP 800-53.

Effective Management of Risk (Challenge 2)

The RG 5.71 states that no matter what mitigation strategy a nuclear power plant decides to implement when applying security controls, the outcome must be that threat and attack vectors associated with the corresponding security control(s) are addressed. In other words, licensees

must mitigate risks to digital systems that could adversely impact the plant's ability to perform critical functions necessary to ensure public health and safety. The challenge rests in ensuring that all vectors are identified and addressed and sufficient guidance exists for users to successfully implement their programs.

Workforce Development (Challenge 3)

The NRC joins with other federal agencies in the need for highly skilled, trained and qualified staff and support personnel to carry out the agency's mission-related activities. The unique operating environments and breadth of technologies in use at commercial nuclear power plants demand the need for specialized expertise, as well. As a result, the NRC is aware that workforce development initiatives within the nuclear sector are important to enabling the agency to meet its mission objectives in the near and long-term.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

The greatest challenges to developing a cross-sector standards framework are: (1) avoiding a framework that is overly broad; (2) individuals and organizations often see the problem differently based on awareness of the scope of digital technologies involved, threat characteristics and capabilities, and the extent of training, education and experience within the cybersecurity field; and (3) the need for improved tailoring guidance to address the needs of organizations and industries within the sector and result in effective protections against cyber-based threats.

3. Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

GENERALLY: 51 *Federal Register* (FR) 28044 published 8/4/1986, and 51 FR 30028 published 8/21/1986, 10 CFR Part 50, "Safety Goals for the Operations of Nuclear Power Plants; Policy Statement; Republication," states,

> "This policy statement focuses on the risks to the public from nuclear power plant operation. Its objective is to establish goals that broadly define an acceptable level of radiological risk…..The Commission has established two qualitative safety goals which are supported by two quantitative objectives. These two supporting objectives are based on the principle that nuclear risks should not be a significant addition to other societal risks. The Commission wants to make clear that no death attributable to nuclear power plant operation will ever be 'acceptable' in the sense that the Commission would regard it as a routine or permissible event."

CYBER SECURITY:

Under the NRC cyber security regulatory framework (e.g., cyber security rule at 10 CFR 73.54, RG 5.71, NRC-approved cyber security plans, inspection and oversight) there are provisions for assessing the impact a cyber attack would have on critical digital assets associated with critical plant functions, such as denying access to systems, services, or data; adversely impacting the confidentiality and integrity of data and/or software; and adversely impacting the operation of systems, networks, and associated equipment. If site-specific analysis demonstrates these impacts exist, mitigation strategies defined in RG 5.71 or the licensed utility's NRC-approved

cyber security plan must be implemented to adequately defend these assets from cyber-based attacks, up to and including the design basis threat.

There are differences in how risk identification and management is performed within the nuclear sector compared to other sectors. For example, the characteristics and attributes of the design basis threat (10 CFR 73.1, "Purpose and Scope") that nuclear power plants must defend against are established and defined by the NRC through regulation and guidance. The design basis threat (DBT) includes information pertaining to cyber-based threats; the use and review of the DBT is an ongoing process that utilizes the best available information to identify potential scenarios for consequence and impact evaluation.

The NRC developed and issued a cyber security roadmap (See http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2012/2012-0088scy.pdf) to evaluate the need for cyber security requirements for fuel cycle facilities (FCFs), non power reactors, independent spent fuel storage installations (ISFSIs) and byproduct materials licensees. To date, the staff has conducted assessments at FCFs, non-power reactors, and ISFSIs; a working group is being established for byproduct materials licensees. The implementation of this roadmap will ensure that appropriate levels of cyber security actions are implemented in a timely and efficient manner at all NRC licensed facilities and identify if any program improvements are needed. The remaining answers provided in this document only consider NRC regulated nuclear power plants.

4. Where do organizations locate their cybersecurity risk management program/office?

While not the focus for the framework under development, the NRC's Computer Security Office (CSO) is responsible for planning, directing, and overseeing the implementation of a comprehensive, coordinated, integrated and cost-effective NRC Information Technology (IT) Security Program, consistent with applicable laws, regulations, Commission management initiatives and policies. The CSO is the Agency-level liaison with external entities on mutual IT security interests; formulates and oversees an IT security program budget; and proposes and successfully advocates appropriate Agency-level IT security guidelines.

With respect to cyber security regulations for operating reactors and combined license applicants, this function resides in NRC's Office of Nuclear Security and Incident Response, the primary organization responsible for 10 CFR 73.54. The NRC regulation at 10 CFR 73.54 requires nuclear power plants to incorporate their cyber security programs as a component of their physical protection programs. RG 5.71, which provides one acceptable method for nuclear power plants to meet the 10 CFR 73.54 requirements, defines roles and responsibilities for a Cyber Security Team, but offers flexibility in how this team functions and is managed within the organization. RG 5.71 is a publicly available document

(See http://nrc-stp.ornl.gov/slo/regguide571.pdf). As the NRC implements its Cyber Security Roadmap, the role of NSIR is increasing to address other types of facilities.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

GENERALLY:

Nuclear power plants are designed to be safe and are operated without significant effect on public health and safety and the environment. While no industrial activity is risk free, the likelihood of a nuclear power plant severe accident with a significant amount of radioactivity releases to the public is very small. This is for many reasons, including diverse and redundant barriers and numerous safety systems in the plant; the training and skills of the reactor operators; testing and maintenance activities; and the regulatory requirements and reactor oversight by the NRC.

NRC regulations contain performance criteria and requirements for a nuclear power plant which ensure an acceptable level of plant safety, i.e., an acceptably low level of risk to public health and safety. The regulations are based on sound engineering precepts and the defense-in-depth concept. To assist with license application and review, the NRC has developed a detailed set of RGs and a standard review plan to clarify regulatory requirements and describe practices that satisfy these requirements. In addition, the NRC periodically issues various generic communications to all nuclear power plants to address potential safety concerns.

The NRC Commission issued a policy statement on the use of probabilistic risk assessment (PRA) methods in nuclear regulatory activities. PRA is a methodology that is used to provide a structured analytical process to assess the likelihood and consequences of severe accidents at nuclear power plants.

When the NRC "risk-informs" its regulations, it examines both the probability of an event and its possible consequences to understand its importance (risk). In other words, NRC asks questions about what can go wrong, how likely it is, and what its consequences might be. The answers guide NRC requirements and regulatory attention to the issues that are most important to the health and safety of the public and the environment.

In implementing a risk-informed approach, the NRC considers a set of five key principles:

- Principle 1: Current Regulations Met
- Principle 2: Defense-in-Depth Consistency
- Principle 3: Maintenance of Safety Margins
- Principle 4: Risk-Informed Analysis
- Principle 5: Performance Monitoring

The NRC uses a risk-informed regulatory approach to identify and support additional requirements or regulatory actions, when needed. Risk information can also be used to reduce unnecessary requirements in purely deterministic approaches.

CYBERSECURITY:

In March 2009, the NRC issued a cyber security regulation at 10 CFR 73.54, “Protection of Digital Computer and Communications Systems and Networks” that applies to existing operating power reactor licensees and combined license applicants. 10 CFR 73.54 required operating power reactor licensees to submit a cyber security plan and an implementation schedule to the NRC for review and approval; all operating reactor licensees met this significant milestone. Combined license applicants submit their cyber security plans on a site specific schedule.

10 CFR 73.54 requires nuclear power plants to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks (up to and including the design basis threat as described in 10 CFR 73.1, “Purpose and Scope”). The cyber security plan must describe how the requirements of 10 CFR 73.54 will be implemented and must account for the site-specific conditions that affect implementation. A template for the cyber security plan can be found in RG 5.71, Appendix A.

The NRC has determined that the compromise of critical digital assets (CDAs) associated with critical plant functions (e.g., safety, security, and emergency preparedness) are not acceptable. The NRC selected the NIST SP 800-53, Revision 3, high security control baseline as the starting point for developing its suite of security controls (presented in RG 5.71, Appendices B and C). The NRC tailored the NIST SP 800-53, Revision 3, high security control baseline to account for the unique environment at nuclear power plants.

The NRC published RG 5.71 in 2010 outlining one acceptable method licensees may use to comply with the requirements of 10 CFR 73.54. The RG is based on standards and guidance outlined in NIST SP 800-53, NIST SP 800-82 “Guide to Industrial Control Systems Security,” Department of Homeland Security (DHS) “Catalog of Control Systems Security: Recommendations for Standards Developers,” and standards published by the International Society of Automation (ISA) and Institute of Electrical and Electronics Engineering (IEEE). The RG also includes a cyber security plan template that nuclear power plant licensees can use when developing cyber security plans for review and approval by the NRC. All operating nuclear power plant licensees submitted a cyber security plan to the NRC for review and approval by NRC staff; NRC has approved all submitted cyber security plans.

Once the cyber security program is established and integrated into the site’s physical protection program, the next steps in the RG 5.71 security lifecycle call for evaluating and managing cyber risk through continuous monitoring, cyber security program reviews, change control, and records retention. As stated in the cyber security rule at 10 CFR 73.54, licensees must design their cyber security programs to apply and maintain defense-in-depth protective strategies to ensure the capability to detect, prevent, respond to, mitigate, and recover from cyber attacks. Defense-in-depth strategies represent a documented collection of complementary and redundant security controls that establish multiple layers of protection to safeguard CDAs. Under a defense-in-depth strategy, the failure of a single protective strategy or security control should not result in the compromise of a safety, important-to-safety, security, or emergency preparedness function.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

Internally, the NRC’s CSO has a team responsible for receiving, tracking, monitoring, and reporting NRC computer security incidents; monitoring NRC's IT security vulnerabilities, maintaining an awareness of the threat to NRC's IT infrastructure, and providing appropriate information to senior NRC officials so they maintain up to date awareness of the threat and NRC's vulnerability to that threat. It is our understanding that the focus of the framework under development is not directed at federal IT infrastructure, but rather industry infrastructure within the nuclear sector. Additional information can be provided regarding NRC’s overarching enterprise risk management, including cyber security risk, as needed.

In terms of protections necessary for NRC licensees to adequately defend against the design basis threat defined in 10 CFR 73.1, "Purpose and Scope" the NRC regulations consider cyber and physical security as intrinsically linked. Establishing a plant-wide cyber security program in accordance with 10 CFR 73.54 is a performance requirement for each nuclear power plant's physical protection program.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

If loss or degradation of function of safety, security, emergency preparedness and support systems occurs due to a cyber attack, the health and safety of the public may be at risk. As a result, the NRC RG 5.71 outlines one acceptable method nuclear power plants may use to comply with the requirements of 10 CFR 73.54 and includes a tailored baseline of management, operational, and technical security controls based on those found in NIST SP 800-53, Revision 3. The RG 5.71 is based on standards and guidance outlined by NIST, DHS, ISA and IEEE.

The commercial nuclear power industry also develops industry-specific guidance that is shared, and in some cases submitted to the NRC for review and endorsement. For example, independent of the NRC's development of RG 5.71, the Nuclear Energy Institute (NEI) developed NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6. The NRC staff found NEI 08-09, Revision 6, acceptable for use by industry (Agencywide Documents Access and Management System Accession No. ML101190371) in meeting the requirements set forth in 10 CFR 73.54. This document provides another template that nuclear power plants can use when submitting CSPs to the NRC for review and approval. NEI 08-09, Revision 6, was reviewed to ensure that the document complied with the requirements set forth in 10 CFR 73.54.

Guidelines are also published by industry organizations such as the Nuclear Institute of Nuclear Power Operations and Electric Power Research Institute, among others.

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

The NRC has a comprehensive risk-informed performance-based regulatory framework. 10 CFR 73.54 require nuclear power plants to provide high assurance that digital computer and communication systems and networks associated with safety, security, and emergency preparedness functions are adequately protected against cyber attacks (up to and including the design basis threat as described in 10 CFR 73.1). The NRC published RG 5.71 in 2010 outlining one acceptable method licensees may use to comply with the requirements of 10 CFR 73.54. The RG also includes a cyber security plan template licensees can use when developing cyber security plans for review and approval by the NRC. The cyber security plans describe how the requirements of 10 CFR 73.54 will be implemented and must account for the site-specific conditions that affect implementation. All cyber security plans were reviewed and approved by NRC, and the cyber security plans have been incorporated into the facilities' NRC licenses. The cyber security plans include, for example, performance-based requirements for the following:

- ensuring that critical plant functions are not adversely impacted by a cyber attack

- conducting analysis to determine which digital assets at the plant require protection, referred to as CDAs, and implementing security controls to protect these digital assets
- applying and maintaining defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber-based attacks, such as the following:
  - prompt detection and response to cyber attacks
  - mitigating the adverse impacts and consequences of cyber-based attacks
  - correcting exploited vulnerabilities, and
  - restoring CDAs affected by a cyber attack
- conducting cyber security awareness training for appropriate facility personnel and contractors
- evaluating and managing cyber risks
- conducting cyber security evaluations for asset modifications
- developing and maintaining written documentation and procedures for cyber security plan implementation
- incorporating the cyber security program as a component of the plant's physical protection program

In addition, NRC's regulatory framework includes an oversight program, consisting of inspection programs and enforcement mechanisms. The inspection programs ensure consistency with the NRC cyber security regulation and a significance determination process to evaluate and disposition inspection findings. The NRC's Enforcement Policy explains the policies and procedures in initiating enforcement actions and the responsibilities of the presiding officers and the Commission in reviewing these actions
(see http://pbadupws.nrc.gov/docs/ML1234/ML12340A295.pdf).

The NRC has requirements in place for different types of event reporting. Reporting requirements focused on cyber security events are currently being developed, pending finalization of the 2011 proposed Enhanced Weapons, Firearms Background Checks, and Security Event Notifications Requirements (*Federal Register*, 76 FR 6200). In the interim, the NRC issued IA-13-01, "Information Assessment Team Advisory for Power Reactors; Updated Criteria to Reporting Suspicious Activity Associated with Cyber Security Incidents" on January 25, 2013. The purpose of this advisory is to provide further guidance on licensee suspicious incident reporting guidelines for cyber security incidents and cyber threat information. This document is not publically available.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

The Nuclear Sector has identified interdependencies with other critical infrastructure sectors, including:

- Chemical as a consumer of hazardous chemicals at fuel cycle facilities;
- Communications as a consumer of services, including cellular towers, central offices, and other critical communications facilities as needed for emergency preparedness functions;
- Energy as a supplier of electricity to the nation's electrical grid;
  - In 2009, the NRC and the Federal Energy Regulatory Commission signed a Memorandum of Agreement (MOA). The purpose of the MOA is to facilitate interactions between the two agencies "on matters of mutual interest pertaining to

the nation's electric power grid reliability and nuclear power plants, including but not limited to coordination of activities related to cyber security." In regards to NRC cyber security inspections, any critical digital asset or critical system that is within the scope of 10 CFR 73.54 is subject to NRC inspection. The NRC staff will share relevant operating experience and other related technical information with NERC regarding these inspections.

- Healthcare and Public Health as a supplier of nuclear medicine, radiopharmaceuticals and in the sterilization of blood and surgical supplies;
- Information Technology as a consumer of critical control systems and services, physical architecture and Internet infrastructure; and
- Transportation Systems through the movement of radioactive materials

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

The NRC established its regulatory requirements for reactor, materials, and waste applications to ensure that "no undue risk to public health and safety" results from licensed uses of facilities and materials covered by the Atomic Energy Act. The NRC's requirements ensure that there is a low probability of accidents that could adversely affect the health and safety of the public.

The regulations set forth in 10 CFR 73.54 establish an overall performance-based requirement for nuclear power plants to ensure that the functions of digital computer and communication systems and networks are protected from cyber attack. A performance-based regulatory approach is one that establishes performance and results as the primary basis for regulatory decision-making, and incorporates the following attributes: (1) measurable (or calculable) parameters (i.e., direct measurement of the physical parameter of interest or of related parameters that can be used to calculate the parameter of interest) exist to monitor system, including facility and licensee performance, (2) objective criteria to assess performance are established based on risk insights, deterministic analyses and/or performance history, (3) licensees have flexibility to determine how to meet the established performance criteria in ways that will encourage and reward improved outcomes; and (4) a framework exists in which the failure to meet a performance criterion, while undesirable, will not in and of itself constitute or result in an immediate safety concern.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

N/A

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

The NRC has a comprehensive oversight process which serves as its conformity assessment mechanism. The oversight process consists of inspections programs and enforcement mechanisms. The inspection programs ensure consistency with the NRC cyber security regulation and a significance determination process to evaluate and disposition inspection findings. The NRC's Enforcement Policy explains the policies and procedures in initiating

enforcement actions and the responsibilities of the presiding officers and the Commission in reviewing these actions (see http://pbadupws.nrc.gov/docs/ML1234/ML12340A295.pdf).

In developing and maintaining its oversight process, the NRC has interacted and reviewed conformity assessment programs and methodologies from both national and international regulators. There is value in exchanging approaches and tools with other similar organizations. Therefore, national and international standards and organizations should play a significant role in formulating a range of options for critical infrastructure cybersecurity conformity assessment tools and mechanisms consistent with the goals of the Framework. As such, we recommend that details of NRC's oversight process be considered to inform the development of conformity assessment approaches for the Framework.

Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage. Please provide information related to the following:

1. What additional approaches already exist?

The NRC approach includes issuing performance-based regulations (10 CFR 73.54) and then providing detailed guidance (RG 5.71) on an acceptable way to meet the intent of the regulation. This approach enables the NRC to provide stability in the regulatory framework, and flexibility in the implementing guidance. The NRC published RG 5.71 in 2010, outlining one acceptable method nuclear power plants may use to comply with the requirements of 10 CFR 73.54. The RG is based on standards and guidance outlined in NIST, DHS, ISA and IEEE.

2. Which of these approaches apply across sectors?

In support of its cyber security regulations, NRC published RG 5.71 specifically for nuclear power plants and where applicable, the NRC staff tailored the security controls in NIST SP 800-53, Revision 3 to the unique environments at these plants. The NRC's efforts to tailor the NIST high baseline security controls are consistent with the recommendations provided in Appendix I to NIST SP 800-53 and in NIST SP 800-82. However, lessons learned from NRC's efforts to develop a comprehensive approach could inform similar developments in other sectors.

Specific elements of the NRC regulatory framework should be considered for application across sectors, including the following:

- Performance-based regulation
- Stable regulatory framework with flexible implementing guidance
- Identify digital assets that must be protected (e.g., safety, security, emergency preparedness functions)
- Defense-in-depth protective strategies
- Application of security controls to digital assets
- Submission of cyber security plan for review and approval

3. Which organizations use these approaches?

10 CFR 73.54 and RG 5.71 apply to operating nuclear power plants licensed by the NRC in accordance with 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," and combined license applicants under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." Owners and operators of nuclear power plants bear the responsibility for assessing and managing the potential for adverse effects on safety, security, and emergency preparedness functions posed by cyber-based attacks so as to provide high assurance that critical functions are adequately protected.

The NRC developed and issued a cyber security roadmap (http://www.nrc.gov/reading-rm/doc-collections/commission/secys/2012/2012-0088scy.pdf) to evaluate the need for cyber security requirements for FCFs, non power reactors, ISFSIs and byproduct materials licensees. To date, the staff has conducted assessments at FCFs, non-power reactors, and ISFSIs; a working group is being established for byproduct materials licensees. The implementation of this roadmap will ensure that appropriate levels of cyber security actions are implemented in a timely and efficient manner at all NRC licensed facilities and identify if any program improvements are needed.

4. What, if any, are the limitations of using such approaches?

The RG 5.71 framework offers operating nuclear power plants and combined license applicants the ability to address the specific needs of a new or existing system. The goal of this regulatory guide is to harmonize the well-known and well-understood set of security controls (based on NIST cyber security standards), guidance, and best practices that address potential cyber risks and provide a flexible programmatic approach in which the plants can establish, maintain, and successfully integrate these security controls into a site-specific cyber security program. The extent to which NRC regulations define the scope of each plant's cyber security program, however, is limited to the agency's regulatory jurisdiction over commercial nuclear facilities as defined by the Atomic Energy Act of 1954, amended in 1974, for matters related to the protection of public health and safety, promotion of common defense, and protection of the environment.

5. What, if any, modifications could make these approaches more useful?

Threat vectors or vulnerabilities tolerated in typical business and governmental computing environments do not exist in the environments where critical digital assets reside. As a result, NIST guidance could be further enhanced with respect to how a facility could address security controls within industrial control environments. In many cases, NRC's robust programmatic requirements (which are conditions for the plant's ongoing operations) offer the option for

implementing alternate or enhanced cyber, or cyber-related, protections for critical digital assets at industrial facilities when the original control cannot be applied as written. Additional guidance would be helpful in aiding these facilities in determining alternative methods for addressing a security control and ensuring these alternatives provide equal or greater protection as the corresponding control. In all instances, more information regarding the purpose and intent for each NIST security control item, and appropriate enhancements, would be useful in evaluating and determining the extent to which a control's purpose and intent are met through alternative measures.

6. How do these approaches take into account sector-specific needs?

10 CFR 73.54 and RG 5.71 apply to nuclear power plants licensed by the NRC in accordance with 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," and combined license applicants under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." Nuclear power plants bear the responsibility for assessing and managing the potential for adverse effects on safety, security, and emergency preparedness so as to provide high assurance that critical functions are adequately protected from cyber attacks.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

As an independent regulatory agency, the NRC takes an active role in the President's Open Government Initiative, with its focus on open, accountable, and accessible government. The NRC has a long history of, and commitment to, transparency, participation, and collaboration in our regulatory activities. That being said, a voluntary program is not applicable to NRC and the commercial nuclear power industry, as NRC regulations are requirements binding on all persons and organizations who receive a license from NRC to use nuclear materials or operate nuclear facilities. NRC is participating in the Executive Order effort and at this time, we believe the NRC's cyber security regulation for operating reactors and combined license applicants meet the intent of the President's Executive Order.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

The NRC participates in the nuclear sector coordinating council and interacts with the sector-specific agency (i.e., DHS). The sector coordinating councils provide a mechanism for interagency interactions and coordinated formulation of issues and actions. As the framework is developed, these sector coordinating councils will provide forums to exchange ideas and best practices on cyber security.

9. What other outreach efforts would be helpful?

The NRC currently coordinates with Federal partners and international stakeholders on cyber security issues through a variety of technical meetings, working groups, workshops, standards development efforts, and conferences.

The NRC regularly reviews and provides comments on international cyber security documents, such as the International Atomic Energy Agency's Nuclear Security Series documents and the International Electrotechnical Commission's cyber security documents, and continues to make a concerted effort to coordinate with the international nuclear community regarding cyber security.

The NRC also regularly participates in interagency working groups, such as the Industrial Control Systems Joint Working Group and the Cross-Sector Cyber Security Working Group, both established by DHS. Furthermore, the NRC regularly participates in industry working groups, such as the Cyber Security Task Force led by the Nuclear Energy Institute (NEI).

Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- ***Separation of business from operational systems;***
- ***Use of encryption and key management;***
- ***Identification and authorization of users accessing systems;***
- ***Asset identification and management;***
- ***Monitoring and incident detection tools and capabilities;***
- ***Incident handling policies and procedures;***
- ***Mission/system resiliency practices;***
- ***Security engineering practices;***
- ***Privacy and civil liberties protection.***

1. Are these practices widely used throughout critical infrastructure and industry?

Yes, all of the bulleted items above, with the exception of privacy and civil liberties protection, are elements contained within RG 5.71, which provides one method acceptable to the NRC for licensees to meet the 10 CFR 73.54 requirements. The NRC regulation at 10 CFR 73.54 requires nuclear power plants to incorporate their cyber security programs as a component of their physical protection programs. RG 5.71 includes a cyber security plan template for use by nuclear power plants to submit for NRC review and approval, as required by 10 CFR 73.54.

Independent of the NRC's development of RG 5.71, the Nuclear Energy Institute (NEI) developed NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6. The NRC staff found NEI 08-09, Revision 6, acceptable for use by industry (ADAMS Accession No. ML101190371) in meeting the requirements set forth in 10 CFR 73.54. This document provides another template that many nuclear power plants used when submitting CSPs to the NRC for review and approval. NEI 08-09, Revision 6, was reviewed to ensure that the document complied with the requirements set forth in 10 CFR 73.54.

2. How do these practices relate to existing international standards and practices?

NRC participates in multilateral and bilateral efforts with international regulatory partners, including the International Atomic Energy Agency (IAEA) in developing, among other things, cyber security guidance and framework documents. The NRC also participates in international cyber security standard development efforts with organizations such as the International Electrotechnical Commission. Interactions such as these allow NRC to participate in facilitated discussions on the development and integration of cyber security programs into existing frameworks; gain a better understanding of what our international partners are doing in regards

to cyber security to ensure early alignment between the United States and other programs; and explain to our international partners what the NRC is doing to address cyber security.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

Interim cyber security milestones were identified for all operating nuclear power plants that emphasized the completion of a set of prioritized activities by December 31, 2012, in order to provide for an appropriate level of cyber protection. All requirements must be addressed by nuclear power plants to ensure high assurance of adequate protection from cyber-based attacks. In addition to the practices listed above, there are many other areas covered by our program that would be equally measured.

4. Are some of these practices not applicable for business or mission needs within particular sectors?

N/A - Requirements for privacy and civil liberties protection are outside scope of NRC regulations.

4. Which of these practices pose the most significant implementation challenge?

Challenges associated with the implementation of NRC cyber security regulatory requirements will vary by site due to the technology in use at these sites and differing facility designs across the nuclear power industry.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

To the extent these practices are addressed by NRC regulations, regulatory guidance, or plant-specific cyber security plans that have been approved by the NRC, with the exception of privacy and civil liberties protection all will be implemented by nuclear power plants and inspected by the NRC. Furthermore, the NRC RG 5.71, which outlines one acceptable method nuclear power plants may use to comply with the requirements of 10 CFR 73.54, is based on standards and guidance outlined by NIST, DHS, ISA and IEEE.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

N/A – The allocation of business resources by the owner and operator of a nuclear power plant is outside the regulatory jurisdiction of the NRC.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

The NRC regulation at 10 CFR 73.54 requires nuclear power plants to incorporate their cyber security programs as a component of their physical protection programs. Cyber security programs include measures for incident response, security assessment and authorization, and security assessment and risk management. The NRC has many methods for sharing security information with the regulated community, including issuance of Information Notices and sharing documents via a Protected Web Server. The PWS is hosted by the NRC to provide documents on suspicious incident reporting, including cyber security, and threat-related documents. The NRC also formed a cyber assessment team (CAT) to provide a consistent process for evaluation and resolution of issues with potential cyber security-related implications for all NRC licensees. The CAT is staffed by experts in cyber security, digital instrumentation and control, and other disciplines from across the agency. These experts support the NRC and its mission by promptly addressing, assessing, and evaluating cyber security-related issues that could impact the NRC licensees' computers, communication systems, and networks associated with safety, security, and emergency preparedness functions. The CAT provides recommendations and/or a course of action to the appropriate program office and NRC management. In accordance with the National Cyber Security Incident Response Plan, the NRC CAT coordinates and communicates with the DHS Industrial Control Systems Cyber Emergency Response Team and the US-CERT on a regular basis.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

None – NRC's cyber security regulations do not implicate privacy and civil liberties issues as 10 CFR 73.54 does not require any private data, such as personal identifiable information, be reported to NRC.

10. What are the international implications of this Framework on your global business or in policymaking in other countries?

N/A – As an independent regulator, the NRC does not have global business interest and is not involved in policymaking in other countries. NRC does participate in multilateral and bilateral efforts with international regulatory partners, including working with the IAEA in developing, among other things, cyber security guidance and framework documents.

11. How should any risks to privacy and civil liberties be managed?

N/A

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

N/A