The first two questions are outside the purview of the NRC, so efforts were directed towards answering the third question, “Has your Commission issued any orders, decisions, or opinions addressing cyber or physical threats since 2001? If so, please provide a brief summary of the deicisons, orders, or opinions?”

In response to the terrorist attacks of September 11, 2001, and subsequent information provided by intelligence and law enforcement agencies, the NRC issued several orders:

- NRC Order EA-02-026, “Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants,” in February 2002 to address the threat environment at the time, including specific requirements that directed nuclear power plant licensees to address cyber and physical security program aspects.

- NRC Order EA-02-261, “Access Authorization Order” in January 2003 to introduce additional criteria for granting unescorted access to nuclear facilities.

- NRC Order EA-03-038, “Fitness for Duty Requirements” in April 2003 to establish work hour control requirements for security personnel at nuclear power plants.

- NRC Order EA-03-039 “Security Personnel Training and Qualification Requirements” April 2003 to establish additional requirements that enhanced the level of training received by security personnel at nuclear power plants.

- NRC Order EA-03-086, “Design Basis Threat for Radiological Sabotage,” in April 2003 to supplement the design-basis threat for nuclear power plants as specified in 10 CFR 73.1 and, in part, added new cyber attack characteristics that a licensee was required to address.

The material aspects of these orders are withheld from public disclosure in accordance with 10 CFR 73.21, “Protection of Safeguards Information: Performance Requirements,” 10 CFR 73.22, “Protection of Safeguards Information: Specific Requirements,” and 10 CFR 73.23, “Protection of Safeguards Information—Modified Handling: Specific Requirements.”

In recognition of the potential cyber security-related issues resulting from the increased use of digital technology at nuclear power plants, in October 2004 the NRC published NUREG/CR-6847, “Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants.” Using NUREG/CR-6847 and insights gained during its development, the Nuclear Energy Institute (NEI) developed NEI 04-04, “Cyber Security Program for Power Reactors,” to provide nuclear power reactor licensees a means for developing and maintaining a cyber security program at their sites. The NRC staff evaluated the NEI submittal and, by letter dated December 23, 2005, informed NEI that NEI 04-04, Rev. 1 provided an acceptable approach to formulate an interim cyber security program in lieu of comprehensive regulatory requirements from the NRC.

In January 2006, the NRC published Regulatory Guide (RG) 1.152, Revision 2, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants.” This regulatory guide provided specific cyber security guidance for nuclear power plant licensees in the development and implementation of protection measures for digital instrumentation and controls used in safety-related applications. The guidance addressed aspects of the implementation of cyber security measures within safety systems that were not adequately covered in Institute of Electrical and

Electronics Engineers (IEEE) Standard 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

In March 2007, the NRC released Branch Technical Position (BTP) 7-14, Revision 5, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems." BTP 7-14, Revision 5, provided review guidelines for evaluating software life cycle processes associated with safety-related digital instrumentation and control systems at nuclear power plants. It also addressed the various characteristics that should be present in an acceptable software management plan.

In January 2007, the Commission approved 10 CFR 73.1, the Design Basis Threat (DBT) Rulemaking, which amended regulations governing the requirements pertaining to the DBT to explicitly include cyber attack. The goal of this rulemaking was to incorporate the requirements put in place by the security Orders, implement aspects of the Energy Policy Act of 2005, and capture lessons learned through implementation and force-on-force evaluations.

In March 2009, the NRC published an updated 10 CFR Part 73. In 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks," nuclear power plant licensees are required to implement a cyber security program to provide high assurance that safety, security, and emergency preparedness functions of nuclear facilities are protected from cyber attacks. In 10 CFR 73.55(b), "Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage," the Commission established requirements for the physical protection program of a nuclear power reactor facility. This includes performance criteria for detecting, assessing, interdicting, and neutralizing threats up to and including the design basis threat of radiological sabotage, as defined in 10 CFR 73.1.

Subsequent to the publication of the new 10 CFR Part 73 rule, the NRC published seven (7) regulatory guidance documents that provide further insights into the details of the physical protection requirements within the new regulation and demonstrate acceptable methodologies for implementation. These regulatory guides include the following:

- RG 1.214, "Response Strategies for Potential Aircraft Threats,"
- RG 5.54, "Standard Format and Content of Safeguards Contingency Plans for Nuclear Power Plants,"
- RG 5.66, "Access Authorization Program for Nuclear Power Plants,"
- RG 5.74, "Managing the Safety/Security Interface,"
- RG 5.75, "Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities,"
- RG 5.76, "Physical Protection Programs at Nuclear Power Reactors," and
- RG 5.77, "Insider Mitigation Program."

Draft RG 5.71, "Cyber Security Programs for Nuclear Facilities," was developed in August 2009 to provide guidance to applicants and licensees on satisfying the requirements of 10 CFR 73.54. The information contained within this guide embodies the findings by standards organizations such as the International Society of Automation, the IEEE, and NIST, as well as guidance from

the Department of Homeland Security (DHS). Draft RG 5.71 describes an acceptable cyber attack protection strategy that consists of a defensive architecture and a set of security controls that are based on NIST SP 800-53, “Recommended Security Controls for Federal Information Systems and Organizations” and NIST SP 800-82, “Guide to Industrial Control Systems Security.” Where applicable, the NRC staff tailored the security controls for the unique environments of nuclear facilities.

Additional details about how NRC has been addressing cyber and physical threats since 2001 are provided in “Protecting Our Nation Since 9-11-01: A Report of the U.S. Nuclear Regulatory Commission” (NUREG/BR-0314), which can be found on the NRC website at http://www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0314/