

# I. Nuclear Energy

*M. Stanford Blanton*

A. Introduction .....	1
B. Post-9/11 Regulatory Process .....	2
C. Facility Physical Security .....	3
D. Information Security .....	8
E. Controlling Access .....	10
F. Security During Construction .....	12
G. Conclusion .....	13

## A. INTRODUCTION

In a departure from its previous reports, the Nuclear Energy Committee has focused its 2010 report on security regulations applicable to commercial nuclear power plants. The report describes the evolution of the Nuclear Regulatory Commission’s (NRC) security regulations since the terrorist attacks of September 11, 2001. Nuclear plants have long been one of, if not the most, heavily secured types of industrial facility in the country. After the 9/11 terrorist attacks, regulators faced a daunting task: how to make security regulations that were already extremely robust, detailed, and capital intensive, even more robust and more detailed, and at the same time maintain reasonable divisions of responsibility among civilian security forces, law enforcement, and the military. For the NRC, like other government agencies, the post-9/11 changes have brought specific new security challenges as well. On the one hand, nuclear facilities are privately owned, and in most respects are operated like any other utility asset, with an eye towards costs and revenues and providing reliable power. On the other, nuclear facilities contain components that in certain circumstances can become targets for a terrorist attack. As the NRC fashioned security regulations, regulators had to reconsider the balance between a nuclear facility’s obligation to protect its own and the government’s larger obligation to national security. As the 2010 report explains, NRC security regulations have been enhanced in several areas since 9/11, the division

---

M. Stanford Blanton is a partner in the Birmingham, Alabama, office of Balch & Bingham LLP, and chair of the Nuclear Energy Committee. The committee gratefully acknowledges the contributions of Chad Pilcher and Millie Ronnlund of Balch & Bingham LLP, who drafted the report; and David Repka and Tyson Smith of Winston & Strawn LLP, who shared their paper “Safeguarding Nuclear Power from Intentional Aircraft Attacks.”

of responsibility for security has been reassessed and continues to evolve, and new frontiers of protection are in the beginning stages.

The scope of NRC security regulations has historically been all-encompassing, generally covering restricted data, national security information, classified information, the storage and transportation of special nuclear material, physical security of facilities, safeguards information, facility security, and employment clearance. Prior to the 9/11 attacks, the NRC's comprehensive security regulations required a written security plan. Access control measures were also already in place, including employee background checks, safeguards access control, and limited physical access to the facility. The facilities themselves employed vehicle barriers and armed security forces, and those armed forces engaged in force-on-force drilling with graded performance. As these examples illustrate, virtually every aspect of a facility's interaction with the outside world is touched by the NRC, and the depth of this oversight only intensified after 9/11.

## **B. POST-9/11 REGULATORY PROCESS**

Although the fundamentals of security regulation remained the same, 9/11 prompted a hard look at security in certain categories. Given the urgency of these issues, the NRC took prompt action. In February 2002, the NRC issued letter orders to every commercial nuclear power plant in the country.<sup>1</sup> These orders generally required increased patrols, augmented security forces and capabilities, additional security posts and physical barriers, vehicle checks at greater standoff distances, enhanced coordination with law enforcement and military authorities, and more restrictive site access controls. Following this first step, the NRC issued similar sets of directives to other facilities, including decommissioned facilities, storage facilities, and enrichment facilities. In April 2003, the NRC issued two new orders. One dealt with additional measures related to security force personnel fitness for duty and security force work hours.<sup>2</sup> The other order added enhanced training and qualification program requirements for armed security personnel, such as including security drills and exercises and more frequent firearms training and qualification.<sup>3</sup>

The new security focus led to revisions to the design basis threat (DBT) regulations, new rules related to aircraft impact and the protection of spent fuel, en-

---

1. See Letter, Issuance of Order for Interim Safeguards and Security Compensatory Measures for [Plant Name] (Feb. 25, 2002) (available in the NRC's public document room, Accession No. ML020510637). Each plant was sent this letter with an attached order, but the orders are not publicly available because they are safeguards information.

2. Order Modifying Licenses (effective immediately) (Apr. 29, 2003) (available in the NRC's public document room, Accession No. ML030940198).

3. See Letter, Issuance of Order for Compensatory Measures Related to Training Enhancements on Tactical and Firearms Proficiency and Physical Fitness Applicable to Armed Nuclear Power Plant Security Force Personnel (Apr. 29, 2003) (available in the NRC's public document room, Accession No. ML030910625). The order is not available because it is safeguards information.

hanced screening for construction and employee forces, intensified protection of safeguards information, and new regulations that aim to address cybersecurity. The earlier orders and the NRC's experience in the years following 9/11 eventually led to major rulemakings: Final Rule Revising Design Basis Threat Regulations (January 2007);<sup>4</sup> Final Rule Revising Protection of Safeguards Information Regulations (October 2009);<sup>5</sup> Final Rule Revising Power Reactor Security Requirements (March 2009);<sup>6</sup> and Aircraft Impact Rule (June 2009).<sup>7</sup>

As a preliminary matter, before delving into a more detailed look at these enhanced regulations, it may be helpful to understand nuclear security regulation by dividing it into three basic categories. Facility physical security involves responding to external threats (e.g., group of armed gunmen or car bomb). Information security refers to regulations that protect sensitive information from external use, including the traditional practices of protecting documents from public disclosure and cybersecurity. The third area, access control, protects both the physical and information aspect of a nuclear plant from internal threats by screening the people who are allowed access to the facility or to certain information.

### C. FACILITY PHYSICAL SECURITY

The NRC regulates based on the concept of the design basis threat (DBT), which refers to the "general adversary characteristics that designated licensees must defend against with high assurance."<sup>8</sup> The defense will involve both the design features of the plant and defensive forces. In April 2003, the NRC issued a set of orders on DBT, separately but simultaneously with the other orders described above, after extensive deliberation and stakeholder input.<sup>9</sup> The push to revise the DBT heated up in 2005 when Congress called for revisions in the Energy Policy Act. When the final DBT rule was published in March 2007, NRC Chairman Dale Klein commented, "This rule is an important piece, but only one piece, of a broader effort to enhance nuclear power plant security. Overall we are taking a multifaceted approach to security enhancements in this post 9/11 threat environment, and looking at how best to secure existing nuclear power plants and how to incorporate security enhancements into design features of new reactors that may be built in coming years." The NRC continues to conduct periodic threat reviews, so the concept of the DBT is not static but responsive to changes in technology and emerging new threats.

---

4. Design Basis Threat, 72 Fed. Reg. 12,705 (Mar. 19, 2007).

5. Protection of Safeguards Information, 73 Fed. Reg. 63,545 (Oct. 24, 2008).

6. Power Reactor Security Requirements, 74 Fed. Reg. 13,926 (Mar. 27, 2009).

7. Consideration of Aircraft Impacts for New Nuclear Power Reactors, 74 Fed. Reg. 28,112 (June 12, 2009).

8. 72 Fed. Reg. 12,705.

9. See Letter, Issuance of Order Requiring Compliance with Revised Design Basis Threat for Operating Power Reactors (Apr. 29, 2003) (available in the NRC's public document room, Accession No. ML030740002). The order is not available because it is safeguards information.

The DBT contained in the March 2007 final regulation begins by requiring consideration of attacks from a certain class of potential adversaries. Licensees should presume that any adversary is armed, has military training, attacks with a kill-or-be killed mentality, and has knowledge of his target—in other words the adversary has “sufficient knowledge to identify specific equipment or locations necessary for a successful attack,” or may have the assistance of individuals on the inside.<sup>10</sup> The DBT goes on to require that the licensee defend against attacks from these kinds of individuals that may come in several different forms. Attacks may be at one or several points of entry each with one or more individuals involved, and adversaries may employ tools like vehicle explosives (in land- or water-borne vehicles), either alone or in conjunction with an external assault, along with various other tools and weapons. The rule specifies that the licensee defend against automatic weapons equipped with silencers, attackers carrying incapacitating agents, and attackers with the tools to force entry into or otherwise destroy the reactor or container integrity, among other possible targets.<sup>11</sup> Along with these various and detailed direct physical characteristics of attack, the DBT requires that the licensee defend against these attacks in conjunction with a cyberattack. The rule presumes that this cyberattack would give the adversary “[t]he capability to exploit site computer and communications system vulnerabilities to modify or destroy data and programming code, deny access to systems, and prevent the operation of the computer system and the equipment it controls.”<sup>12</sup> In defending against all the possible iterations of such an attack, the licensee must also consider that the attack may come by force (e.g., violent external assault), by stealth, or by deceptive action (e.g., diversionary tactics). The DBT presumes that the goal of these attacks, and so the overall threat that licensees are protecting against, is radiological sabotage or theft of strategic special nuclear material (SNM).<sup>13</sup>

In considering the intensity of the DBT, it is hard not to think of licensee security forces like military personnel—after all, security forces at plants are expected to defend against adversaries trained and equipped in large part like military combatants. Understandably, as the DBT rule was being considered, comments raised the possibility of federalizing plant security forces. More generally, comments noted that the NRC’s statements in the DBT did not clearly articulate when an attack on a facility crossed from being a private security force issue to being a national security issue that the federal government forces should be responsible for diffusing.<sup>14</sup> The NRC soundly rejected the idea of federalizing security forces and explained its view of how a threat greater than anticipated by the DBT would be handled. The NRC “expect[s] that, if confronted by an adversary beyond its maximum legal capabilities, onsite security would continue to respond with a graded reduction in effectiveness. The Commission is confident that a licensee’s

---

10. 72 Fed. Reg. 12,723.

11. *Id.*

12. *Id.*

13. 72 Fed. Reg. 12,722–23.

14. 72 Fed. Reg. 12,713–14; 12,719–20.

security force would respond to any threat no matter the size or capabilities that may present itself.”<sup>15</sup> In other words, while the NRC explained that federal and local authorities will be called upon to respond, there is no clear demarcation for telling licensees when their responsibility ends, “In the Commission’s view, establishing set boundaries demarcating [between the licensee and the government] is neither possible nor desirable.”<sup>16</sup> However, despite this expectation that private security forces will defend to their maximum capability, the DBT rule’s requirement is limited to threats “a private security force can reasonably be expected to defend” against.<sup>17</sup>

One threat that the NRC did consider specifically was air-based attacks. The NRC determined an air-based attack was a “beyond-[DBT] event”<sup>18</sup> that licensees should not be required to defend against:

Ultimately, the Commission has determined that active protection against the airborne threat requires military weapons and ordnance that rightfully are the responsibilities of the Department of Defense (DOD), such as ground-based air defense missiles, and thus, the airborne threat is one that is beyond what a private security force can reasonably be expected to defend against. This does not mean that the Commission is discounting the airborne threat; merely that the responsibility for actively protecting against the threat lies with other organizations of the Federal government . . .<sup>19</sup>

As is clear from the NRC’s discussion, while there is not a bright line separating private from governmental security obligation, the NRC does envision a division of responsibilities. The government’s realm of responsibility definitely includes protection from aircraft assault, protection from missiles, and U.S. defense activities.<sup>20</sup> However, the NRC did explain that not all activity by an enemy of the state is beyond-DBT. The adversaries contemplated under the DBT rule may be enemies of the state, although their attack falls within the DBT. Rather, licensees are not required to defend against enemies of the state when to do so would require weaponry reserved for U.S. military or other law enforcement authority, making the division of responsibility dependent on the attack, not on the identity of the attacker.<sup>21</sup> Put simply, adversaries, vehicles and equipment that can be actively engaged by the licensee’s security force are included within the licensee’s realm of responsibility.<sup>22</sup>

---

15. 72 Fed. Reg. 12,714.

16. *Id.*

17. 72 Fed. Reg. 12,713.

18. Consideration of Aircraft Impacts for New Nuclear Power Reactors, 74 Fed. Reg. 28,112 (June 12, 2009).

19. 72 Fed. Reg. 12,710.

20. 72 Fed. Reg. 12,714–15.

21. *Id.*

22. *Public Citizen v. NRC*, 573 F.3d 916, 924 (9th Cir. 2009) (“Though the scope of the DBT has not previously been precisely defined, the NRC’s decisions have clearly been animated by considerations of the credibility of the threat at issue and whether private forces can reasonably be expected to

Although the NRC has ruled that aircraft attacks are not the licensee's responsibility to defend against, there are other safeguards that help to protect against the effects of such an attack. In the Aircraft Impact Rule,<sup>23</sup> the NRC set out the requirement that applicants for new plants conduct an aircraft impact assessment. New plant applicants must "[u]sing realistic analyses, identify and incorporate into the design those design features and functional capabilities to show, with reduced use of operator action, that the facility can withstand the effects of an aircraft impact . . . [and] [d]escribe how such design features and functional capabilities show, with reduced use of operator action, that the facility can withstand the effects of an aircraft impact."<sup>24</sup> In sum, new plants must consider in their application how an impact would affect key safety functions, including core cooling capability, containment, spent fuel cooling capability, and spent fuel pool integrity, although assumptions the licensee must consider like type of aircraft, speed, and angle of impact are not publicly available. If the design cannot show a practical way to maintain these key safety functions after an impact, the applicant must consider other design options.<sup>25</sup> Of course, licensees are required to "identify actions to mitigate the effects of large fires and explosions, including those caused by aircraft impacts."<sup>26</sup> Additionally, it is worth noting that nuclear plants already have a rugged design, with the reactor protected by a thick layer of concrete, making penetration by aircraft difficult at the outset.

Aircraft and other terrorist attacks have also been discussed in the context of environmental reviews under the National Environmental Policy Act (NEPA). The NRC's categorical finding that a NEPA review did not require consideration of terrorist attacks was based on the risk of a terrorist attack being too far removed from the action of licensing a nuclear facility, that the risk could not be determined, that NEPA did not require a worst case scenario analysis, and that the NRC public process was not the appropriate forum for sensitive security issues. This finding was later challenged, and there is currently a split among the U.S. Circuit Courts of Appeal for the Ninth and Third Circuits. The Ninth Circuit found that the NRC's rule was unreasonable because the NRC considered terrorist attacks in other contexts,<sup>27</sup> while the Third Circuit found otherwise because there was no reasonably close causal relationship between licensing a facility and the environmental effects of a terrorist attack.<sup>28</sup>

All commercial nuclear plants must plan for the storage of spent nuclear fuel, the uranium-bearing fuel elements that have been used at commercial nuclear reactors but are no longer producing enough energy to sustain a nuclear reaction.

---

actively engage that threat. This rationale, while not previously articulated in any one section of the rule, is easily ascertained from the history and context of the DBT rule." (citations omitted)).

23. Consideration of Aircraft Impacts for New Nuclear Power Reactors, 74 Fed. Reg. 28,112 (June 12, 2009).

24. 74 Fed. Reg. 28,118.

25. 74 Fed. Reg. 28,119.

26. 74 Fed. Reg. 28,115 (citing 10 CFR 50.54(hh)).

27. *San Luis Obispo Mothers for Peace v. NRC*, 449 F.3d 1016 (9th Cir. 2006).

28. *N.J. Dep't of Env'tl. Prot. v. NRC*, 561 F.3d 132 (3d Cir. 2009).

The two acceptable methods for storing the spent fuel after it is removed from the reactor core are by use of spent fuel pools and dry cask storage. Spent fuel pools are structures constructed of thick, steel reinforced concrete walls with stainless steel liners located inside of protected areas. The spent fuel rods are stored under at least twenty feet of water, and the spent fuel pools may be shielded by other structures, including intervening walls that would obstruct the impact of other objects.<sup>29</sup> Dry cask storage allows spent fuel that has already been cooled in the spent fuel pool for at least one year to be surrounded by inert gas inside a steel cylinder container. Each dry cask cylinder is surrounded by additional steel, concrete, or other material to provide radiation shielding to workers and members of the public. The casks are designed to resist floods, tornadoes, projectiles, and temperature extremes.<sup>30</sup>

In order to meet the objectives for the safe storage of spent nuclear fuel, the operators of a nuclear power plant are required to store the spent nuclear fuel in a protected area, and access to the protected area may only be granted to authorized individuals.<sup>31</sup> A plant must be able to detect and assess any unauthorized access to or activities within the protected area, must provide timely communication to a designated response force whenever necessary, and must manage the physical protection organization in a manner that maintains its effectiveness.<sup>32</sup> In addition, the spent nuclear fuel must be protected by two physical barriers, one barrier at the perimeter of the protected area and another barrier offering substantial resistance to potential outside penetration. The perimeter of the protected area is constantly observed by surveillance and is monitored by an active intrusion alarm system that can detect any penetration into the isolation zone.<sup>33</sup> The primary alarm system must be located within the protected area; have bullet-resistance walls, doors, ceiling, and floor; and may not be visible from outside of the protected area.<sup>34</sup> All individuals, vehicles, and packages entering the protected area must be checked for proper authorization and visually searched for explosives prior to entry.<sup>35</sup> The licensee is required to keep detailed documentation about who is granted access to the protected area, screening of those individuals, logs of all security patrols, alarm records, and physical protection program reports.<sup>36</sup>

SNM includes plutonium, uranium-233, uranium enriched in the isotopes uranium-233 or uranium-235, or any other material that the Commission may determine to be such SNM. Uranium-233 and plutonium are not produced naturally, but both can be formed in nuclear reactors and can be extracted from spent fuel by chemical separation. SNM is only mildly radioactive, but it includes some fissile

---

29. See [www.nrc.gov/waste/spent-fuel-storage/pools.html](http://www.nrc.gov/waste/spent-fuel-storage/pools.html).

30. See [www.nrc.gov/waste/spent-fuel-storage/dry-cask-storage.html](http://www.nrc.gov/waste/spent-fuel-storage/dry-cask-storage.html).

31. 10 C.F.R. § 73.51(b)(2)(i)–(ii).

32. 10 C.F.R. § 73.51(b)(2)(iii)–(v).

33. 10 C.F.R. § 73.51(d)(3).

34. *Id.*

35. 10 C.F.R. § 73.51(d)(9).

36. 10 C.F.R. § 73.51(d)(13).

material—uranium-233, uranium-235, and plutonium-239—that, in concentrated form, can be the primary ingredients of nuclear explosives. Therefore, the federal government has placed special emphasis on the control of this special nuclear material.<sup>37</sup>

In order to meet the NRC's general performance objectives and requirements for the transport of SNM, an in-transit physical protection system must restrict access to and access in the vicinity of transports and strategic SNM. To achieve this capability, the physical protection system must minimize the vulnerability of the strategic SNM by using preplanning itineraries for the movement of SNM, periodically updating knowledge of route conditions, maintaining knowledge of the status and position of the SNM while en route, and determining and communicating alternative itineraries as conditions warrant.<sup>38</sup> The protection system should also be able to detect and delay any unauthorized attempt to use stealth or force to gain access to or introduce unauthorized materials into the vicinity of transports and strategic SNM. This can be done by using controlled access areas to isolate strategic SNM and transports to assure that unauthorized persons shall not have direct access to the transports and strategic SNM and by using access detection subsystems and procedures to assess and inform of any unauthorized penetration of a controlled access area.<sup>39</sup> Additionally, the protection system should be able to detect any attempts to gain unauthorized access or to introduce any unauthorized materials into the vicinity of the transports by using deceitful tactics.<sup>40</sup> Finally, the in-transit physical protection system must prevent or delay any unauthorized entry or attempt to introduce unauthorized materials into strategic SNM from a transport (or attempting the unauthorized removal of such material).<sup>41</sup>

The protections described above may be accomplished by responding to safeguards, contingencies, and emergencies that may arise and by engaging and impeding adversaries until local law enforcement forces arrive.<sup>42</sup> In order to rapidly and effectively respond to any situations that may occur, the transport should include a security organization composed of trained and qualified personnel. The security force should possess a predetermined plan to respond to safeguards and contingency events. It also should have access to both equipment and procedures for its protection and communications equipment that will allow them to rapidly and accurately transmit security information.<sup>43</sup>

#### D. INFORMATION SECURITY

The NRC must protect classified and sensitive unclassified information related to government programs for the physical protection and safeguarding of nuclear

---

37. See [www.nrc.gov/materials/sp-nucmaterials.html](http://www.nrc.gov/materials/sp-nucmaterials.html).

38. 10 C.F.R. § 73.25(b)(1).

39. 10 C.F.R. § 73.25(b)(2).

40. 10 C.F.R. § 73.25(b)(3).

41. 10 C.F.R. § 73.25(c).

42. 10 C.F.R. § 73.25(d).

43. 10 C.F.R. § 73.25(d)(1), (2).

materials or facilities to ensure that such information is protected against unauthorized disclosure. Safeguards information (SGI) is a special category of sensitive unclassified information that was authorized to be protected by Section 147 of the Atomic Energy Act. SGI concerns the physical protection of operating power reactors, spent fuel shipments, strategic special nuclear material, or other radioactive material, but it is handled in a similar manner as classified information.<sup>44</sup>

A licensee that produces, receives, or acquires SGI must ensure that it is protected from unauthorized disclosure.<sup>45</sup> To achieve this goal, those in possession of SGI must establish and operate an information protection system that includes measures for maintaining SGI that relate to power reactors, the possession and transportation of SNM, fuel fabrication facilities, uranium enrichment facilities, and similar operations.<sup>46</sup> Any safety procedures that are implemented by federal, state, or local law enforcement agencies are presumed to meet the general performance requirements,<sup>47</sup> but the NRC possesses the authority to impose different or more stringent protections for SGI.<sup>48</sup>

The information that must be protected as SGI includes site specific drawings, diagrams, sketches, maps, alarm system layouts, physical security orders and procedures, lock combinations, mechanical key design, passwords, and the size and arrival times of response forces.<sup>49</sup> No one may be granted access to SGI unless that person has undergone an FBI background check and been deemed as having a “need to know” the information.<sup>50</sup> When matters containing SGI are in use, they must be under the control of an individual who is authorized to access SGI. SGI information within alarm stations or rooms that are continuously occupied by authorized individuals is not required to be stored in a locked security container.<sup>51</sup> When SGI is unattended, it must be stored in a locked security container that does not identify the contents, and only a select group of individuals is permitted to know the lock combinations for accessing SGI.<sup>52</sup> Any document or other matter containing SGI must be marked conspicuously on the top and bottom of each page.<sup>53</sup> SGI may be transported externally and stored on a stand-alone computer, but specific, stringent procedures must be followed for its handling.<sup>54</sup>

Another major concern for the NRC is an attack on the cybersecurity of nuclear facilities and material. Therefore, the Commission has taken action to enhance the protection of the facilities’ computer systems. Importantly, electronic information systems that operate nuclear power plants and other safety equipment are isolated from the Internet as an added layer of protection from outside intrusions. Also,

---

44. See [www.nrc.gov/security/info-security.html](http://www.nrc.gov/security/info-security.html).

45. 10 C.F.R. § 73.21(a)(1).

46. 10 C.F.R. § 73.21(a)(1)(i).

47. 10 C.F.R. § 73.21(a)(2).

48. 10 C.F.R. § 73.21(b).

49. 10 C.F.R. § 73.22(a)(1).

50. 10 C.F.R. § 73.22(b)(1).

51. 10 C.F.R. § 73.22(c)(1).

52. 10 C.F.R. § 73.22(c)(2).

53. 10 C.F.R. § 73.22(d).

54. 10 C.F.R. § 73.22(f), (g).

each licensee is required to submit a cybersecurity plan that includes a proposed implementation schedule and provides high assurance that digital computer and communication systems and networks are adequately protected against cyberattacks.<sup>55</sup> Specifically, the licensee must protect digital computer and communication systems and networks concerning safety-related functions, security functions, emergency preparedness, and any support systems or equipment.<sup>56</sup>

In addition, the licensee must analyze computer and communications systems, identify those assets that must be protected from cyberattacks, and incorporate the cybersecurity program into the physical protection program.<sup>57</sup> The cybersecurity program must be designed to implement security controls to protect the computer systems of the licensee, apply and maintain in-depth defense strategies, and ensure the capability to respond to any such attack.<sup>58</sup> Further, the program must ensure that the appropriate personnel are properly trained to perform any necessary tasks associated with the cybersecurity program.<sup>59</sup>

In March 2009, FERC issued Order 706-B, which explained that while the NERC Critical Infrastructure Protection (CIP) Reliability Standards exempted nuclear power facilities, NRC regulations do not extend to all equipment within a nuclear power plant.<sup>60</sup> FERC traditionally possessed jurisdiction over transmission lines, but Order 706-B requires that any “balance of plant equipment” that is not regulated by the NRC to be covered by FERC. In January 2010, the NRC signed a memorandum of understanding with NERC regarding the enforcement of NRC cybersecurity regulations and CIP Reliability Standards.<sup>61</sup> For cybersecurity inspection protocol, the NRC has the responsibility for inspecting those digital assets that affect safety, security, and emergency preparedness functions of a nuclear power plant. The NRC does not have regulatory responsibility to inspect digital assets unrelated to these functions unless those systems have an adverse effect on those same functions. NERC has regulatory responsibility for inspecting digital assets related to the continuity of power for compliance with NERC’s CIP standards. NRC and NERC agreed to share any information that is discovered during the course of their respective inspections that may be relevant or have an adverse impact on any digital asset governed by the other agency’s security requirements.<sup>62</sup>

## E. CONTROLLING ACCESS

In accordance with NRC guidelines, each licensee for a nuclear power plant licensed under 10 C.F.R. Part 50 is required to conduct screening of individuals

---

55. 10 C.F.R. § 73.54(a).

56. 10 C.F.R. § 73.54(a)(1).

57. 10 C.F.R. § 73.54(b).

58. 10 C.F.R. § 73.54(c).

59. 10 C.F.R. § 73.54(d).

60. Order No. 706-B, Mandatory Reliability Standards for Critical Infrastructure Protection, 126 FERC ¶ 61,229, Docket No. RM06-22 (Mar. 19, 2009).

61. See [www.nerc.com/files/NERC-NRC%20MOU%2020091230%20executed.PDF](http://www.nerc.com/files/NERC-NRC%20MOU%2020091230%20executed.PDF).

62. *Id.*

who will be granted unescorted access to the facility. This screening process is referred to as the “access authorization program” (AAP), and the nuclear power plant is required to develop, implement, and maintain the program in order to protect against a threat at the plant from an insider. The AAP helps to protect the plant by ensuring that each person who is granted access to the facility is trustworthy and reliable, does not constitute an unreasonable risk to the health and safety of the public or the common defense and security, and does not pose a threat to either interrupt the normal operations of the plant or commit radiological sabotage.<sup>63</sup>

After 9/11, the NRC advised its licensees to assume a heightened level of awareness with regard to access authorization at nuclear power plants. The NRC began comprehensive reviews of its safeguards and security programs, and on January 7, 2003, implemented measures to enhance the AAP in 10 C.F.R. § 73.56. There have been several updates and amendments to this program since that time, and the security orders have now been aligned with the requirements in 10 C.F.R. § 73.56, thereby enabling the NRC to achieve stability in its regulation, increase the effectiveness of the program, clarify the existing regulatory requirements, and codify the requirements in one location.<sup>64</sup>

AAPs also apply to those people whose duties and responsibilities permit them to take actions by electronic means that could impact the plant’s operational safety, security, or emergency preparedness; individuals who implement a plant’s protective strategy; and employees of contractors or vendors who are working for the facility.<sup>65</sup> The operator of a nuclear power plant must review the following information before an individual is granted unescorted access to an NRC-licensed facility: employment history, military history, criminal history, credit history, education history, interviews with provided references, initial drug and alcohol screening, and an initial psychological screening.<sup>66</sup> Once an individual is granted access to the facility, he or she is still subject to being observed by a supervisor trained to detect any changes in behavior that could result in degraded or impaired performance.

The licensee must also conduct follow-up and random drug testing as part of its AAP. First, the NRC requires companies that operate nuclear power plants to have a fitness for duty (FFD) program that requires testing for behavior that could affect the safety or security of the plant, including, but not limited to, drug or alcohol abuse, and arrests, indictments, or court mandated alcohol or drug programs. Individuals may also be subject to a behavioral observation program, which requires employees to report evidence of drug or alcohol abuse, illness, behavioral changes, and aberrant behavior.

In accordance with 10 C.F.R. Part 26, certain NRC-regulated facilities are required to implement FFD programs. The purpose of an FFD program is to provide reasonable assurance that nuclear facility personnel are trustworthy, will perform

---

63. See [www.nrc.gov/reactors/operating/ops-experience/access-authorization.html](http://www.nrc.gov/reactors/operating/ops-experience/access-authorization.html).

64. *Id.*

65. 10 C.F.R. § 73.56(b).

66. See generally 10 C.F.R. § 73.56.

their tasks in a reliable manner, are not under the influence of any legal or illegal substance that may impair their ability to perform their duties, and are not mentally or physically impaired in a manner that could adversely affect their ability to safely and competently perform their duties.<sup>67</sup> Behavioral observation programs are instituted in order to detect behaviors that may indicate the possible use, sale, or possession of illegal drugs, the use or possession of alcohol on site or while on duty, or the impairment from fatigue or any cause that, if left unattended, may constitute a risk to public health and safety or the common defense and security. Any individual who is subject to a behavioral observation program must report FFD concerns about other employees to the appropriate personnel.<sup>68</sup>

## F. SECURITY DURING CONSTRUCTION

The development of the next generation of nuclear plants has accelerated since 2001, and as a result, physical security begins before a nuclear plant ever has nuclear material or produces the first megawatt. The NRC is in the process of developing new regulations governing security during the construction phase, and has issued a preliminary proposed rulemaking entitled Access Authorization and Physical Security for Nuclear Power Plant Construction.<sup>69</sup> These changes would affect portions of 10 C.F.R. Parts 50, 52, and 73. The rule would require a written construction security plan with the objective “to provide assurance that malicious acts during construction cannot later reasonably result directly or indirectly in radiological sabotage.”<sup>70</sup> The new rule would divide the construction process into four phases. Phase 1 begins with the pouring of structural concrete excluding the base mat and would require background checks and a behavioral observation program for certain construction forces, security patrols, and a construction site security force.<sup>71</sup> Phase 2 begins with onsite in-place security- or safety-related systems, structures, or components. In addition to the security requirements in Phase 1, Phase 2 would require more access control and additional vehicle and individual search requirements to deter the introduction of firearms, explosives, and incendiary devices.<sup>72</sup> Phase 3 encompasses the transition to the physical security plan, which would remain in effect throughout the plant’s operation. In addition

---

67. 10 C.F.R. § 26.23.

68. 10 C.F.R. § 26.33.

69. Available in the NRC’s public document room, Accession No. ML100750461. According to the NRC staff presentation at the March 31, 2010, public meeting regarding the draft language, the recommended proposed rule language is planned to be submitted to the Commission for approval in August 2010, with formal publication of the proposed rule to follow. *See* Access Authorization & Physical Security during Nuclear Power Plant Construction Draft Proposed Rule Meeting Slides for March 31, 2010 Category 3 Workshop (available in the NRC’s public document room, Accession No. ML100880240).

70. Access Authorization and Physical Security for Nuclear Power Plant Construction, § 10 C.F.R. § 73.52(c) (proposed).

71. 10 C.F.R. § 73.52(d)(1) (proposed).

72. 10 C.F.R. § 73.52(d)(2) (proposed).

to the security requirements in the earlier phases, Phase 3 would require security sweeps, lockdown of controlled access construction areas, barriers to deter and delay unauthorized penetration attempts, and some enhanced surveillance and monitoring.<sup>73</sup> Phase 4 would simply require that the licensee cease following the requirements of the construction security rule and implement its operational security program.<sup>74</sup> Additionally, the draft language would contain more stringent access requirements, such as demographic checks. NRC staff is also considering stakeholder input regarding whether to include a fingerprinting requirement.

## G. CONCLUSION

As the NRC continues to assess security issues, the regulations already strengthened after 9/11 will continue to evolve. As technology improves, licensees may be expected to take on an even greater role in defending against external threats, and it is certain that cybersecurity and security during construction will be subject to intense scrutiny in the near term. Commercial nuclear power is enjoying a renaissance, but is also facing what could be called the most burdensome and intense security regulation in U.S. history. The NRC continues to wrestle with this tension and hopes to work with licensees in their efforts to comply and to participate in the regulatory process so that the industry can continue to produce clean energy safely and efficiently.

---

73. 10 C.F.R. § 73.52(d)(3) (proposed).

74. 10 C.F.R. § 73.52(d)(4) (proposed).

