(U) Some Alternative Staff Views

(U) INTRODUCTION:

(U) The purpose of this enclosure is to present the views of some of the U.S. Nuclear Regulatory Commission (NRC) staff with regards to reasonable assurance of protection time (RAPT) and security bounding time (SBT) concepts, particularly with respect to time to core damage (TTCD). These staff include all of the security risk analyst subject matter experts currently performing target set inspections (14 total) and some security and resident inspectors in the regions (hereafter referred to as "these technical staff").

(U) The cover SECY paper provides the Commission with two concepts (RAPT and site-specific SBT) for crediting beyond-design-basis event response strategy equipment, offsite response that includes law enforcement and off-duty licensee personnel (security and operations).

(U) These technical staff's preference is that rather than providing regulatory relief for those target sets that have a longer TTCD, that credit could be provided in an equally beneficial way without removing regulatory compliance of equipment that a licensee may no longer identify as a target set. This method would not require changes to the current target sets and would instead address the significance of potential findings that result in longer TTCDs by creating new enforcement guidance. Additionally, credit for operator actions that can be accomplished with the assistance of law enforcement response could be provided in the context of force-on-force (FOF) inspections, when the additional operator actions can mitigate the loss of a target set. This would allow for licensees to demonstrate and receive credit for those additional actions that could be utilized after a loss of target set, to mitigate the effects of significant core damage. This would foster additional training opportunities for the licensee to perform and coordinate these actions and ensure compliance with the site's ability to prevent significant core damage with reasonable assurance.

(U) DISCUSSION:

(U) Target Sets

(U) Target sets are the foundation upon which a licensee builds its protective strategy. In accordance with the statements of consideration (SOC), target sets are defined as the "…minimum combination of equipment or operator actions which, if prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant core damage… barring extraordinary actions by plant operators."[1] In addition, the SOC describes "extraordinary actions" as those actions that do not meet the following criteria: (1) sufficient time is available to implement these action; (2) environmental conditions allow access where needed; (3) adversary interference is precluded; (4) any equipment needed to complete these actions is available and ready for use; (5) approved procedures exist which have entering conditions outside of severe accident mitigation guidelines (SAMG) or equivalent, and; (6) training is conducted on the existing procedures under conditions similar to the scenario assumed. Target sets were not intended to comprise an exhaustive list of ways a licensee can

[1] (U) Statement of Considerations for Power Reactor Security Requirements Final Rule, dated March 27, 2009: https://www.govinfo.gov/content/pkg/FR-2009-03-27/pdf/E9-6102.pdf

(U) prevent significant core damage, but rather, the minimum list of equipment, and by implication, the most risk-significant.

(U) Target sets are a key element in the design of licensees' protective strategies. With implementation of RAPT, a licensee can remove elements from target sets, and under site-specific SBT, a licensee can either remove or add elements. The elements removed are no longer identified as a target set element and, therefore, the regulations that apply to target set elements would no longer be applicable. Specifically, elements that are no longer designated as target set elements would no longer be subject to the requirements of Title 10 of the *Code of Federal Regulations* (10 CFR) paragraphs 73.55(b)(4), 73.55(f)(3), and 73.55(f)(4) or subject to random patrols in accordance with 10 CFR 73.55(76)(5)(vi). For example: today, licensees can be cited for a failure to analyze a target set in accordance with 10 CFR 74.55(b)(4); however, using the concept of RAPT or site-specific SBT, once an element is no longer identified as a target set element based on TTCD or law enforcement response, an inspector may no longer have a basis or regulatory requirement to challenge a licensee.

(U) With a site-specific SBT, an action that previously would be identified as an "extraordinary action" rather than a target set element, could now be identified as a target set element itself. For example, consider a site that has a target set containing two elements—A and B. These two elements are plant equipment identified as equipment which, if prevented from performing their intended safety function or prevented from being accomplished, could lead to significant core damage, barring extraordinary actions by plant operations. Using the site-specific SBT, a licensee could add equipment that requires an action taken by an operator such as tying in standby equipment from a FLEX facility located in the owner-controlled area. This would likely require recalled site personnel or law enforcement to protect operator movement and/or to clear the area of explosives, and thus could result in a lengthy task time. This equipment, along with the associated actions, would create Element C and designate it as part of the minimum combination. Element C would only be utilized by operations to prevent significant core damage if Elements A and B were destroyed and, therefore, should not be considered part of the minimum combination. In most cases, destruction of Elements A and B would require an adversary to have penetrated the site's protected area. These elements that require extraordinary actions may involve actions being taken under unknown, untested, and unpredictable hostile action scenarios. For these reasons, these technical staff believe that elements such as Element C – that require extraordinary actions – should not drive the design of the protective strategy. In these technical staff's opinion, that could divert security resources from the protection of the elements that provide more certainty in preventing significant core damage. Therefore, these technical staff believe it would be more appropriate for a licensee to receive credit for extraordinary actions by demonstrating the ability to perform them at appropriate times (e.g., after Elements A and B are compromised) during NRC-conducted FOF exercises.

(U) <u>Today's Target Set Program</u>

(U) Today, target set inspectors use an 8-hour TTCD as a determination for if a performance deficiency is more-than-minor. Based on current documentation, all but three reactor sites screen out or no longer identify target sets with a TTCD of 8 hours, and document these screened-out elements as "additional considerations." The additional considerations section in a target set book identifies anything above and beyond the minimum combination of equipment or actions that a licensee may have available to mitigate, not prevent, significant core damage, such as extraordinary actions or items identified in SAMGs. During an NRC-conducted FOF inspection, only the equipment or actions identified as target set elements are used – this does

(U) not include anything listed under the additional considerations section. The purpose of differentiating between a target set element and additional considerations is to ensure a license is considering and/or protecting the most significant equipment to prevent significant core damage. If equipment identified as additional considerations were part of the minimum combination of a target set, there is the potential that every piece of equipment and action available on and offsite would be tested during an FOF. This path negates the point of having target sets in the first place, as they are intended to focus on a minimum, risk significant combination. In addition, recent violations for target set deficiencies are cited for the licensee's failure to analyze target set equipment, not the failure to meet a specific timeline (i.e. 8 hours). Currently, the 8-hour criterion is used by NRC inspectors to provide consistency between regional target set findings when determining significance, after a performance deficiency is identified. This method allows NRC inspectors a regulatory hook if licensees screen out target set elements that a licensee is required to consider in the design of their protection strategy. Specifically, 10 CFR 73.55(f)(1) requires licensees to identify target sets and 10 CFR paragraphs 73.55(b)(4) and 75.55(f)(3) require licensees to consider or account for target sets in the design of their protection strategy. If TTCD is used to no longer designate equipment as target set elements under RAPT or SBT, these regulations would no longer be applicable. Technical staff do not believe that TTCD calculations should be able to provide regulatory relief from 10 CFR paragraphs 73.55(f)(1), 73.55(f)(3), and 73.55(f)(3). Technical staff agree that the 8-hour criteria should be documented; however, its ability to remove regulatory requirements associated with target set elements should not qualify as risk-informed. Technical staff agree that if a TTCD calculation was standardized as a condition to utilize RAPT, then RAPT is a viable option. However, due to the complexity associated with both standardizing a definition and methodology to identify TTCD, and the significant inspection effort it would take for an inspector to verify these calculations, technical staff believe there are other paths that put less reliance on TTCD and provide more credit to licensees.

(U) Front-line Systems

(U) These technical staff agree that licensees should continue to design their physical protection programs to address the security of the principal systems (front-line), such as high-pressure injection, reactor core isolation cooling/isolation condenser, auxiliary/emergency feedwater and continue to scope-in these systems and equipment in the target sets regardless of the TTCD determined for these systems and equipment. However, they disagree that batteries, fuel sources, or component cooling, should not also continue to be scoped-in along with the front-line systems. These components, in their view, are automatic actions that are not based on the availability of operator actions. If these components are made inoperable, with time and/or immediately, the front-line systems may not be able to maintain reactor coolant inventory following a loss of coolant accident, decay heat removal following a reactor trip or loss of main feedwater or providing emergency AC power following a loss of plant off-site power. Their view is that excluding this equipment as part of front-line systems would be inconsistent with how the NRC already defines system operation. For example, the NRC template for standard technical specifications defines operability as:

> (U) A system, subsystem, train, component, or device shall be OPERABLE or have OPERABILITY when it is capable of performing its specified safety function(s) and when all necessary attendant instrumentation, controls, normal or emergency electrical power, cooling and seal water, lubrication, *and other auxiliary equipment that are required for the system, subsystem, train, component, or device to perform its specified safety function(s) are also capable of performing their related support function(s).*

(U) These technical staff believe licensees are already appropriately identifying the sub-components required to ensure target set equipment can perform its function and have already removed the sub-components that are only required for longer TTCD scenarios. Re-defining an area that licensees are already implementing well, as evident by lack of target set findings and/or violations in this area, seems unnecessary to these technical staff and is unclear how a distinction is drawn between what a "component" of a front-line system is versus "equipment supporting the operation of these systems."

(U) For example, there are systems where battery power is required to start and/or align injection pathways for the front-line systems. If the RAPT concept allows removal of these systems as target set elements, it has the potential to challenge the ability of a licensee to design their physical protection program.

(U) The cover SECY paper also discusses how inclusion within a target set can be based on the availability of operator actions that can be performed after an associated RAPT or SBT. Credible operator actions were established to ensure licensees receive credit in target sets. These technical staff consider the SECY paper's discussion to be somewhat redundant because operator actions are not currently required to be part of a target set and are, therefore, a licensee's preference to include them or not. In the end, both current practice and the application of RAPT allows exclusion of operator actions.

(U) RAPT's Alternative Approach to Regulatory Guide (RG) 5.81, Revision 1, "Target Set Identification and Development for Nuclear Power Reactors"

(U) The SECY paper states that RAPT addresses an alternative method that allows a licensee to maintain only the front-line systems to direct focus on the more risk-significant target set elements; however, RG 5.81 already provides guidance for a licensee to direct focus on the more risk-significant systems and is utilized by some licensees. Specifically, Section 5.9, "Alternate Approaches," of RG 5.81 states:

> (U) While the assumed goal of the adversary is to disable a complete target set, the goal of the physical protection program and protective strategy is to ensure that at least one element of each target set remains in order to prevent the adversary from achieving its objective. This goal can be achieved by protecting each target set, *or by protecting a set of equipment derived from the target sets that includes one element from each target set.*

(U) The only difference between current guidance provided in RG 5.81 and RAPT is in the identification of target set elements. RAPT allows a licensee to no longer designate equipment and/or actions as target set elements if TTCD is greater than 8 hours and document these equipment or actions in a different section of the target set book, such as additional actions. RG 5.81, Section 6, "Screen for Achievable Target Set Elements," states that achievable target set elements are those that are within the capabilities of a DBT adversary to compromise, destroy, or render nonfunctional, independent of response strategy. Despite the differences in designation of target set elements noted above, both current guidance and the RAPT concept allow a licensee to focus and design their protective strategy to prevent significant core damage based on what is considered the most risk-significant equipment.

(U) Time to Core Damage

(U) These technical staff believe that, after reviewing licensees' target sets the NRC has on file for FOF planning purposes, the 8-hour RAPT will not allow for removal of target sets without licensees recalculating TTCD. In the view of these technical staff, risk-informing actions are predicated on plant design and the SECY paper departs from that concept by allowing licensees to determine what TTCD means. These technical staff believe that under the RAPT or site-specific SBT, that relies on TTCD calculations, TTCD will now have a major role in ensuring a licensee is accounting for target sets in the design of the physical protection program and ultimately, the need for compliance with 10 CFR paragraphs 73.55(b)(4), 73.55(f)(3), and 73.55(f)(4).

(U) For example, in 2019, an inspection team questioned the validity of a target set for which the licensee identified two elements, referred to here as Element A and Element B. Based on the inspector's knowledge, the loss of Element A alone could result in significant core damage. In order to evaluate this condition, the licensee simulated the loss of Element A in the simulator and the onset of core damage occurred in 6.5 hours. However, the site also provided a modular accident analysis program (MAAP) with a TTCD of greater than 17 hours. NRC staff reviewed the MAPP run the licensee provided and identified multiple errors on the licensee's inputs and assumptions. The NRC's effort to validate the licensee's TTCD calculations took multiple weeks to assess and disposition this minor violation for failure to analyze this condition in accordance with 10 CFR 73.55(b)(4). The intent of this example is to highlight that verifying TTCD is a very resource intensive effort for both the NRC and licensee. Additionally, no matter what criteria or methodology the licensee uses to determine TTCD, there is no regulatory requirement that an inspector can cite for non-conservative or inadequate TTCD calculations. Under the RAPT, the licensee could choose to use the 17-hour TTCD and remove it as a target set – resulting in paragraphs 73.55(b)(4), 73.55(f)(3), and 73.55(f)(4) of 10 CFR no longer being applicable.

(U) Modes of Operation

(U) The SECY paper makes statements related to a number of target set elements decreasing in lower modes of operation. These technical staff believe that if a target set is achieved by an adversary, equipment may not be available to reach or remain in a lower mode of operation. Due to radioactive decay, the fuel in the reactor will continue to generate a significant amount of heat. If cooling fails due to target set destruction, heat can increase the fuel temperature to the point of damaging the reactor. As temperature and pressure rise, a licensee may not be able to inject with lower pressure systems, meaning the number of targets available for destruction by an adversary would not decrease in a lower mode.

[redacted]

(U) CONCLUSION:

(U) These technical staff believe that application of RAPT or a site-specific SBT may not consider some equipment in the design of their physical protection program because it will no longer be designated a target set element. These technical staff believe that actions that require extraordinary action can, in some scenarios, be effectively utilized; however, the

(U) availability of this equipment should not dilute the protection of more reliable plant equipment. These technical staff agree in concept with the SECY paper that NRC-conducted FOF exercises should not result in regulatory action if a mock adversary force were to destroy target set elements where a licensee has equipment, e.g., FLEX, to mitigate the loss by use of extraordinary operator actions (e.g., with assistance from law enforcement). In these technical staff's opinion, rather than use of the RAPT or site-specific SBT concepts, the appropriate methodology to increase realism is performance-based testing of these additional actions. Today, licensees do not have to demonstrate performance of additional actions during FOF inspections. As a result, these technical staff believe this potentially enables licensees to overestimate their response capabilities.

(U) Furthermore, these technical staff believe that there may be simpler alternatives that would provide a similar benefit without adding unnecessary risk associated with TTCD. An alternate path forward is to document in Inspection Manual Chapter 0612, Appendix E, "Examples of Minor Issues" that any potential findings resulting from analysis of a target set with a TTCD beyond 8 hours would not meet the criteria for a more-than-minor determination but could still potentially be a minor violation. In these technical staff's view, this would maintain the identification (designation) of target sets as required by 10 CFR paragraphs 73.55(b)(4), 73.55(f)(3) and (f)(1) while still giving licensees the flexibility to choose which target set elements to protect when designing their physical protection program. They believe this will retain the focus for target set consideration on the most reliable equipment, rather than allowing an inconsistent methodology for TTCD to determine what equipment is protected as a target set.

(U) Since the general concept of the RAPT philosophy is supported, in that it would not require any additional regulations, rule changes, or interpretations, it is these technical staff's opinion that if RAPT is implemented, TTCD should be defined. Lastly, at least one method of calculating TTCD should be identified and added to RG 5.81 concurrently with the issuance of RAPT in RG 5.76, "Physical Protection Programs at Nuclear Power Reactors (Safeguards Information)."