September 1, 2015

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Dodaro:

I am responding to your letter, dated June 4, 2015, which called attention to open U.S. Government Accountability Office (GAO) recommendations in three areas that GAO believes the Commission should give high priority to addressing. Those areas are: (1) improve information technology (IT) management, (2) address the security of industrial radiological sources, and (3) improve the reliability of cost estimates. The Commission recognizes your concerns regarding the open recommendations and is taking action to address them, as described below.

Improve IT Management

Regarding improving IT management, you specified that completing the baseline to determine the number, types, and costs of commodity IT investments, as recommended in GAO-14-65, *INFORMATION TECHNOLOGY: Additional OMB and Agency Actions Are Needed to Achieve Portfolio Savings,* would enable the U.S. Nuclear Regulatory Commission (NRC) to identify opportunities for cost savings or cost avoidance. In addition, you specified that developing a comprehensive agencywide policy for managing software licenses, as recommended in GAO-14-413, *FEDERAL SOFTWARE LICENSES: Better Management Needed to Achieve Significant Savings Government-Wide*, would enable NRC to identify opportunities for cost savings or cost avoidance. The NRC agrees that these two fiscal year (FY) 2014 GAO reports contain open recommendations that, if implemented, could help NRC reduce costs and better manage its IT infrastructure.

With respect to developing a complete commodity IT baseline,[1] the NRC is continuing to make progress in centralizing its IT commodity spending. The NRC is also transitioning to a new IT investment classification methodology to better capture and classify IT costs, including commodity IT costs. The NRC is currently re-competing its largest IT services contract to maximize the value and quality of our enterprise-wide services and to identify further consolidation opportunities by May 1, 2017.

With respect to developing an agencywide comprehensive policy for the management of software licenses, the NRC has developed a framework and maturity model for Software Asset Management and is in the process of completing a future state roadmap and activity plan to integrate with the governance, processes and technology relating to the comprehensive strategy. However, NRC's progress has slowed due to funding and staffing reductions.

[1] GAO found that the NRC was one of 12 agencies with partially completed baselines.

Additionally, you called to my attention your concern for NRC's ensuring the security of information systems and cyber critical infrastructure. I assure you that the NRC is strongly engaged in efforts to maintain the security of the agency's information systems, assets and data while protecting privacy. Numerous actions are underway to ensure the agency addresses cybersecurity challenges and mitigates risks. Recent efforts include improving NRC's cybersecurity posture through participation in the 30-day Cybersecurity Sprint activity.

The NRC identified the need to prioritize risk management efforts in order to balance increasing threats and their cybersecurity risk impacts to the NRC mission. For example, in FY 2013, the agency commenced developing and implementing the Cybersecurity Risk Dashboard (CRDB). The CRDB project is a multi-year effort to increase the identification, communication, quantification, and prioritization of strategies to reduce cybersecurity risk and its potential impact to the NRC mission. Dashboards display real time information such as the status of cybersecurity risk management activities, training completion rates, and the pilot cybersecurity performance index (CPI) for NRC offices and regions. The CPI is a metric for quantifying and measuring an organization's cyber performance in an understandable and transparent method using well-known risk drivers. Starting in FY 2016, the NRC plans to implement CPI at the agency level as well as at office and regional levels.

Furthermore, the NRC continues efforts to improve situational awareness. During the past quarter, the NRC notified the U.S. Computer Emergency Readiness Team of computer security incidents within required timeframes 97% of the time. Most importantly, the agency conducts phishing testing on over 90% of its local area network users. Those individuals who succumb to the phishing test are required to take phishing training and are re-tested in the next quarter.

Address the Security of Industrial Radiological Sources

Regarding addressing the security of industrial radiological sources, you encouraged NRC to give high priority to the implementation of two recommendations in GAO-14-293, *NUCLEAR NONPROLIFERATION: Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Sources.* GAO-14-293 Recommendation 2 stated that the NRC should reconsider whether the definition of collocation should be revised for well logging facilities that routinely keep radiological sources in a single storage area but secured in separate storage containers. GAO-14-293 Recommendation 3 stated the NRC should conduct an assessment of the trustworthiness and reliability (T&R) process—by which licensees approve employees for unescorted access—to determine if it provides reasonable assurance against insider threats, including (1) determining why criminal history information concerning convictions for terroristic threats was not provided to a licensee during the T&R process to establish if this represents an isolated case or a systemic weakness in the T&R process; and (2) revising, to the extent permitted by law, the T&R process to provide specific guidance to licensees on how to review an employee's background. The recommendation stated that the NRC should also consider whether certain criminal convictions or other indications should disqualify an employee from being considered trustworthy and reliable or trigger a greater role for NRC in making a T&R determination.

I can assure you that the NRC takes this security effort very seriously, and that all licensees possessing radioactive materials, including those that possess un-collocated quantities of concern that fall outside of the NRC's increased security controls, must maintain constant surveillance and access control to the licensed material to prevent unauthorized removal. The NRC and Agreement States verify that licensees maintain proper security measures for controlling and maintaining access to un-collocated quantities of radioactive material of concern through inspection oversight.

The description of the conviction for "terroristic threats" in the case referenced in GAO-14-293 Recommendation 3 is misleading. During a domestic dispute, the individual verbally threatened two other individuals. It was a misdemeanor on a local law enforcement record, 12 years prior to the request for unescorted access, which was not cited on the FBI record. As a result, the information was not available to support the T&R determination for this individual. This situation does not reflect a performance deficiency or a systemic weakness in the licensee's implementation of the NRC requirements. A criminal history record by itself does not provide sufficient information to determine if an individual is trustworthy and reliable. The FBI criminal history check is only one component of a background check. Licensees must use the information provided in the FBI report in conjunction with information on employment history, personal references and education checks in making a T&R determination.

The NRC has provided licensees specific guidance on making T&R determinations for individuals requiring unescorted access to category 1 and category 2 quantities of radioactive material in NUREG-2155, Rev. 1*, Implementation Guidance for 10 CFR Part 37, "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material"* (January 2015), and NUREG-2166, *Physical Security Best Practices for the Protection of Risk-Significant Radioactive Material* (May 2014).

As part of our commitment to regulatory effectiveness, the NRC reviews its programs to ensure we are regulating in a manner that effectively and efficiently manages known risks and threats, clearly communicates requirements, and ensures that regulations are consistently applied and are practical.

The NRC staff is implementing a comprehensive assessment of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 37 and will provide a report to Congress in December 2016 on its evaluation of the effectiveness of Part 37 security requirements to protect high risk radioactive material. As part of the effectiveness review, the NRC will specifically assess both the definition of collocation of radioactive materials and the T&R process.

The NRC plans to issue a Temporary Instruction (TI) in August 2016, to evaluate T&R determinations during 10 CFR Part 37 security inspections. The TI will be utilized to collect and document specific information on the T&R process in order to determine the effectiveness of licensees' access authorization and background investigation requirements, whether licensees are establishing effective T&R disqualifying criteria, and to determine if enhancements to the T&R process are needed through regulatory guidance, stakeholder outreach, or rulemaking.

Improve the Reliability of Cost Estimates

Regarding improving the reliability of cost estimates, you stated that NRC should align its cost estimating procedures with relevant best practices identified in the *GAO Cost Estimating and Assessment Guide,* as recommended in GAO-15-98*, NUCLEAR REGULATORY COMMISSION: NRC Needs to Improve Its Cost Estimates by Incorporating More Best Practices.* In addition, you stated that GAO-12-258, *NUCLEAR REGULATION: NRC's Oversight of Nuclear Power Reactors' Decommissioning Funds Could Be Further Strengthened,* had also recommended that NRC use GAO's cost estimating characteristics as a guide for a high-quality cost-estimating formula.

The NRC staff is updating its cost-benefit guidance to incorporate feedback provided by licensees, the Nuclear Energy Institute, the GAO, and other stakeholders. These improvements are discussed in the cost-benefit update activities described in the staff's paper, SECY-14-0002, "Plan for Updating the U.S. Nuclear Regulatory Commission's Cost-Benefit Guidance," dated

January 2, 2014 (Agencywide Document Access and Management System Accession No. ML13274A495), which includes a two-phase process for updating the NRC's cost estimating procedures. The first phase of this plan is currently in progress and is expected to culminate with the release of draft guidance for public comment in November 2015. This phase will: consolidate guidance documents; incorporate recommendations from the GAO's 2014 report on the NRC's cost-estimating practices and cost-estimating best practices from the GAO's guide; and capture best practices for the consideration of qualitative factors in accordance with Commission direction in the Staff Requirements Memorandum for SECY 14-0087. A detailed plan and schedule for developing the draft revised guidance is due to the Commission for information in September 2015. As the NRC staff updates these documents, it will engage the Advisory Committee on Reactor Safeguards and the public to ensure meaningful input. The NRC held its first public meeting on its cost-benefit update activities on July 16, 2015, to discuss implementation of the two-phased approach to revise the cost-benefit guidance, including the preliminary schedule for such work.

Until the updated guidance is issued for use, all pending regulatory proposals will be guided by the 2004 guidance document. However, the NRC staff will be applying the improvements in cost estimating and cost-benefit analysis to the pending regulatory proposals as each improvement is adopted.

In summary, the NRC takes each GAO recommendation seriously and implements appropriate corrective actions commensurate with the significance of the recommendation.

If you need any additional information, please contact me or Jesse Arildsen, Office of the Executive Director for Operations, at (301) 415-1785.

Sincerely,

/RA/

Stephen G. Burns

cc: F. Rusco