September 19, 2016

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 July 8, 2016, which called attention to open recommendations that the U.S. Government Accountability Office (GAO) believes the U.S. Nuclear Regulatory Commission (NRC) should prioritize. Those recommendations are related to: (1) information technology (IT) management, (2) the security of industrial radiological sources, and (3) the reliability of cost estimates. The Commission recognizes the GAO's concerns regarding the open recommendations and appreciates GAOs recognition that the NRC is making progress on each recommendation. Please find in the enclosure an update on the actions that NRC is taking to address them.

The NRC appreciates the efforts of GAO to identify opportunities improve operations, takes each GAO recommendation seriously, and plans to implement appropriate corrective actions commensurate with the significance of each recommendation. If you need any additional information, please contact me or John Jolicoeur, Executive Technical Assistant, Office of the Executive Director for Operations at (301) 415-1642.

Sincerely,

/RA/

Stephen G. Burns

cc: M. Gaffigan

NRC Actions to Address Priority Open GAO Recommendations

Improve Information Technology (IT) Management

Regarding improving IT management, GAO 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 US. Nuclear Regulatory Commission (NRC) to identify opportunities for cost savings or cost avoidance. In addition, GAO 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 be similarly beneficial. The NRC agrees that these two open recommendations could help NRC reduce costs and better manage its IT infrastructure.

With respect to developing a complete commodity IT baseline, the NRC's Office of the Chief Information Officer has made significant progress in centralizing IT commodity spending and in capturing information relevant to developing consolidation/shared service plans. NRC has also restructured its IT portfolio to provide greater transparency into IT costs, including commodity IT, and has instituted new internal controls to ensure all IT spending is appropriately captured and categorized. This information lays the groundwork for developing additional consolidation and shared services plans.

With respect to developing an agencywide comprehensive policy for the management of software licenses, the NRC signed a letter of intent on July 19, 2016, to participate in the General Services Administration's Software License Management as a Service pilot program.

Utilizing the expertise captured in this program, the NRC is executing its own Information Technology Asset Management (ITAM) Project with the following objectives:

- Establish a baseline IT asset inventory (both software and hardware).
- Define ITAM framework, governance, policy, processes and procedures that will enable the NRC to achieve cost savings; conduct strategic inventory planning and procurement forecasting; and increase accountability, security, and compliance.
- Establish ownership, roles, and responsibilities of the defined ITAM framework.
- Define tool requirements for centralized, automated tracking, and management of IT assets throughout their lifecycle.
- Define the set of requirements to be included in the performance work statement or statement of work that is determined to be optimal for procuring ITAM integration services.

GAO also expressed concern about the NRC ensuring the security of information systems and cyber critical infrastructure. The NRC continues efforts to ensure the security of its information systems, cyber critical infrastructure, and personally identifiable information. The NRC staff has implemented programs to ensure that the agency has an effective cyber security program to protect and minimize the risk to the NRC's IT assets and systems.

Address the Security of Industrial Radiological Sources

Regarding the security of industrial radiological sources, Recommendations 2 and 3 in GAO-14-293, "Nuclear Nonproliferation: Additional Actions Needed to Increase the Security of U.S. Industrial Radiological Sources," remain open. Recommendation 2 was that the NRC should reconsider whether the definition of collocation (also referred to as "aggregation" in Part 37 of Title 10 of the *Code of Federal Regulations* (10 CFR Part 37), "Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material" should be revised for well logging facilities that routinely keep radiological sources in a single storage area but secured in separate storage containers. Recommendation 3 was that 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. The GAO recommended that the NRC's assessment include: (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 GAO 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 the NRC in making T&R determinations.

Regarding Recommendation 2 on the issue of collocation, current NRC regulations require that all licensees possessing category 1 and 2 quantities of radioactive materials, must implement access controls to prevent unauthorized access or removal of licensed material when it is in storage, and must maintain constant surveillance of material when it is not in storage. The NRC and Agreement States verify that licensees maintain proper security measures for controlling and maintaining access to quantities of radioactive material of concern through inspection oversight. Inspection of collocated sources indicates that appropriate security is being maintained by licensees.

The NRC is currently conducting a comprehensive review of the 10 CFR Part 37 requirements to determine whether any additional security measures, revisions, or additions to guidance rulemaking changes, or licensee outreach efforts are appropriate. A re-evaluation of collocation is included in this effort. The NRC staff is on schedule to provide a report detailing the results of this program review to the Commission later in 2016.

Regarding Recommendation 3, to conduct an assessment of the T&R process, item 1 of Recommendation 3 regarding terroristic threats was addressed in NRC's 2015 update to the status of this recommendation. Regarding item 2 of Recommendation 3 to determine if the T&R requirements provide reasonable assurance against an insider threat.

Currently 10 CFR Part 37 includes T&R requirements to ensure that individuals who have unescorted access to Category 1 and 2 quantities of radioactive material are trustworthy and reliable and do not constitute an unreasonable risk to the public health and safety or security of the radioactive material. Licensees are required to conduct a number of activities pursuant to 10 CFR 37.25 in order to make a T&R determination for unescorted access to Category 1 and 2 quantities of radioactive material. This includes a Federal Bureau of Investigation identification and criminal history records check to determine if an individual has a record of criminal activity; verification of true identity, employment history, and education; and

the conduct of a character and reputation determination. These activities provide the basis for granting or denying an individual unescorted access to Category 1 and 2 quantities of radioactive material. NUREG-2166 provides additional guidance to licensees in conducting T&R evaluations and making T&R determinations.

The NRC's comprehensive review of 10 CFR Part 37 will provide additional insights into the capability of the T&R process to mitigate insider threats and the specificity associated with the NRC's guidance for conducting T&R assessments. Additional insights will be gained through temporary instruction (TI) 2800/042, "Evaluation of Trustworthiness and Reliability Determinations," which the NRC issued to gather specific information regarding licensee T&R programs. The NRC staff expects to complete the TI by November 2016. The results of the TI will be used to determine whether any additional security measures, guidance updates, rulemaking changes, or licensee outreach efforts are appropriate in the area of T&R.

Improve the Reliability of Cost Estimates

Regarding improving the reliability of cost estimates, GAO stated that NRC should align its cost estimating procedures with relevant best practices identified in the *GAO Cost Estimating and Assessment Guide*. In addition, GAO-12-258, "NUCLEAR REGULATION: NRC's Oversight of Nuclear Power Reactors' Decommissioning Funds Could Be Further Strengthened," 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 cost estimating best practices and the treatment of uncertainty to support the development of more realistic estimates of the costs to implement proposed requirements. In addition to GAO input, this guidance is considering relevant best practices and feedback provided by licensees, the Nuclear Energy Institute, and other stakeholders. The cost-benefit guidance update is currently in progress and the NRC expects to release the draft guidance for public comment in early 2017. This update will consolidate guidance documents; incorporate appropriate recommendations and best practices from GAO; and capture best practices for the considering qualitative factors in accordance with Commission direction in the staff requirements memorandum for SECY 14-0087, "Qualitative Consideration of Factors in the Development of Regulatory Analyses and Backfit Analyses". As these documents are updated, the staff will engage the Advisory Committee on Reactor Safeguards and the public.

The NRC staff will be applying the guidance updates in cost estimating and cost-benefit analysis to the pending regulatory proposals as each update is adopted.

The Commission also notes the concerns identified in the area of strategic human capital management. In June 2014 the NRC established Project Aim to enhance the agency's ability to plan and execute its mission while adapting in a timely and effective manner to a dynamic environment. Project Aim included strategies and detailed recommendations to improve the NRC's agility, effectiveness, and efficiency, while also refining the basis for agency planning. Human capital management plays a significant role in Project Aim. The NRC is developing a Strategic Workforce Plan to ensure that the right people with the right skills are in the right place at the right time to achieve the agency's mission.