Joint Statement for the Record

Lisa Casias
Deputy Assistant Secretary for Administration
U.S. Department of Commerce

Dr. Kent Rochford
Acting Undersecretary for Standards and Technology and Director
National Institute of Standards and Technology
U.S. Department of Commerce

Before the
United States House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight
and
Subcommittee on Research and Technology

U.S. Department of Commerce and National Institute of Standards and Technology Response to the Government Accountability Office's Report Entitled: *"Physical Security: NIST and Commerce Need to Complete Efforts to Address Persistent Challenges"*

October 11, 2017

Thank you Chairman LaHood, Ranking Member Beyer, Chairman Comstock, Ranking Member Lipinski, and distinguished members of the Subcommittees. We appreciate the opportunity to appear before you today to discuss the Department of Commerce's response to the recently released report by the Government Accountability Office (GAO) entitled: *"Physical Security: NIST and Commerce Need to Complete Efforts to Address Persistent Challenges."*

The National Institute of Standards and Technology (NIST)'s programs focus on national priorities from advanced manufacturing and the digital economy to precision metrology, quantum science, biosciences, and more. NIST's overall mission is to promote U.S. innovation and industrial competitiveness. NIST does this by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

As this Committee knows, the world-class research conducted at NIST needs world-class facilities to accomplish the NIST mission, but just as important, NIST needs robust, consistent adherence to standards for physical security to ensure that personnel are working in a safe environment and that our assets are protected. We are committed to bringing together all necessary Department resources to achieve that goal.

We welcome the Subcommittees' support of the Department's efforts to continue to improve overall security. The Department continues to take steps to improve the physical security at NIST and throughout the Department, and intends to fully implement the recommendations contained in the GAO report. Specifically, today we will discuss where we are in improving the security culture at both NIST campuses and across the Department, and the steps we have taken to ensure successful implementation of the report's recommendations.

The Office of the Assistant Secretary for Administration (ASA) oversees the Office of Security (OSY). The Secretary of Commerce has delegated authority to OSY to manage and implement all security, emergency management, and threat investigations across the Department and its 13 bureaus and operating units. The OSY's mission is to protect personnel, facilities, and information by collaborating with key leaders, decision-makers, and stakeholders across all of the Department's bureaus and operating units to effectively mitigate security risks throughout the Department.

Responsibility for security does not rest solely with OSY. The head of each operating unit or bureau is responsible for ensuring the security of the personnel, facilities, property, information and assets of their respective organizations in accordance with applicable laws, regulations, Executive Orders, and directives. The Director of Security is responsible for advising and assisting heads of operating units. Thus, NIST's Director shares with OSY the role of protecting the Department's personnel, mission, information, and infrastructure at NIST.

We are committed to a comprehensive assessment of the roles and responsibilities between OSY and NIST at NIST's two campuses, in Gaithersburg, MD, and Boulder, CO, as recommended in the GAO report. Currently, OSY is charged with delivering integrated law enforcement and security services and protection, while NIST is responsible for ensuring the physical security of the buildings. In practice, this means that NIST has primary responsibility for providing and

maintaining electronic locks, surveillance devices, and alarms at NIST's campuses. NIST also is responsible for establishing local campus security procedures, and the maintenance and management of the physical security systems such as access control systems, intrusion detection systems, identification badging, and other security and safety systems designed to protect NIST assets.

In turn, OSY provides the security personnel to monitor security cameras, undertake routine patrols of NIST's campuses and buildings, and provide emergency assistance. It also oversees a contract guard force that staff entry points to the campuses.

OSY manages upwards of 75 security personnel at NIST, utilizing a mix of Police Services Group (PSG) Officers and contract Protective Security Officers (PSO), along with oversight and support staff. The PSG and guard contract delegations were transferred to OSY in November 2015. Pursuant to section 113 of the American Innovation and Competitiveness Act, OSY employs a Director for Security at NIST who supervises the PSG and contract guards at NIST.

NIST takes its responsibility to ensure the physical security of NIST's two campuses very seriously. NIST is working with OSY to strengthen the security culture at NIST, which the GAO notes has already had some success, though there is still more work to be done.

GAO Report

The GAO, at the request of this Committee and the Senate Committee on Commerce, Science, and Transportation, undertook a comprehensive review of the physical security of NIST's campuses in Gaithersburg and Boulder. We appreciate the GAO's efforts as it provides us with important information and an additional perspective as we work to strengthen security across the Department and at NIST.

The GAO's report made four recommendations: two directed primarily to OSY, and two directed primarily to NIST, although both OSY and NIST recognize that we must continue to work together to strengthen security at the campuses. We agree with the GAO's recommendations, and have taken a number of steps to implement them. So far, we have:

- Implemented, through OSY, the requirement that all Security Specialists conducting Facility Security Assessments be trained and certified through the Interagency Security Committee (ISC) Risk Management Process (RMP) in FY17. Beginning in FY18, all DOC Facility Security Assessments will be conducted in accordance with the ISC RMP. In implementing these activities, the Department's Manual for Security Policies and Procedures has been aligned with the ISC RMP. This chapter is currently in the Department's internal clearance process. This update also incorporates all recommended elements from the GAO report related to campus Facility Security Committees, risk decision documentation, and alternative countermeasure recommendations.

- Increased oversight, testing and inspection, both announced and unannounced, of Protective Security Officers. Additionally, Protective Security Officers have also been retrained to reinforce the security posture and effectiveness of security access points at various Department campuses and facilities.

- Through OSY, continued implementation of "Security Awareness Day" across the Department, and specifically at NIST, to increase employee awareness of security, safety and emergency responsibilities, policies, procedures and programs. In fact, the NIST Gaithersburg campus held its Security Awareness Day on October 10 and Boulder campus is scheduled to hold its Security Awareness Day on October 19.

- Dedication by NIST of approximately $4M for physical security programs and systems enhancements, reflecting our commitment to the physical security of NIST campuses, and the ability of NIST personnel to work in a safe environment.

- Developed in 2016 NIST's internal Security Policy. As the GAO report acknowledges, this action and others demonstrated "leadership's commitment to transforming NIST's security culture." The Security Policy is intended to ensure the security of NIST personnel, buildings, and other plant facilities, equipment, property, and assets.

- Established NIST's Security Advisory Board (SAB) in January 2017, which the GAO report observed "affirms the commitment of NIST management to establishing and maintaining a comprehensive, effective, and efficient agency-wide approach to physical security at NIST."

- Initiating the addition of a security element to all NIST employees' performance plans, ensuring that security is afforded the same high level of importance in one's job performance as other elements. This effort and others will drive a culture of change with respect to security.

- Already conducting a "Security Sprint" or a deep dive into NIST's work to prioritize its security needs, applying many of the ISC RMP principles, and developing action items necessary to address those needs. NIST has prioritized the actions and is currently implementing many of these actions. As recommended by GAO, NIST and the Department are incorporating elements of key practices of risk management, as well as interim milestones, into the implementation of the Security Sprint Action Plans.

Finally, the GAO report recommends the Department assess the current security organizational structure between OSY and NIST. The report encourages us "to identify the most effective and feasible approach to physical security at NIST." While each of these entities currently has specific, non-duplicative responsibilities, we recognize that there might be alternative organizational structures that may more effectively promote security. For that reason, the Department is undertaking a comprehensive, holistic assessment of the NIST physical security

organization as recommended by the GAO and will take a fresh look at the most appropriate and effective roles and responsibilities for OSY and NIST to best manage our security challenges.

Secretary Ross is committed to ensuring safety and security across the Department of Commerce. We appreciate the Subcommittees' interest in the Department's ongoing work to improve the physical security at NIST's campuses, and we welcome your questions.