OPENING STATEMENT

RANKING MEMBER PAUL D. TONKO

SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT
HEARING ON

NASA CYBERSECURITY:
AN EXAMINATION OF THE AGENCY'S INFORMATION SECURITY

FEBRUARY 29, 2012

Thank you for calling this hearing Mr. Chairman, and I want to extend a welcome to our two distinguished witnesses this morning. Inspector General Martin has been getting high marks for the work of his office and Ms. Cureton should be congratulated for being willing to take on a tough job that the country needs to see done well.

Twice in 2008 an earth observation satellite managed by NASA's Goddard Space Flight Center experienced several minutes of interference that prevented NASA from communicating with the spacecraft. The events were indicative of an intentional cyber attack and the techniques used were - quote - "consistent with authoritative Chinese military writings," according to a report by the U.S.-China Economic and Security Review Commission. The report did not attribute the specific instances against the NASA satellites to China but the implications were clear: NASA's spacecraft may be vulnerable to acts of cyber attack. In both instances involving NASA's Terra Earth Observation Satellite (EOS), the report concluded – quote: "The responsible party achieved all steps required to command the satellite but did not issue commands."

Cyber attacks against NASA are nothing new. Over the past decade both American citizens and foreign nationals have penetrated the agency's cyber defenses, installed malicious software and stolen scientific, security and other data. These threats have come from foreign nationals in China, Great Britain, Italy, Nigeria, Portugal, Romania, Russia, Turkey and Estonia. Just last month a Romanian national who had allegedly hacked into a NASA computer server and posted sensitive satellite data he acquired on-line was arrested by Romanian officials. Last November, the NASA Office of Inspector General, along with the FBI announced charges against six Estonian nationals and one Russian national for infecting NASA and other computers with malware that secretly altered the settings of more than *four million* infected computers sending Internet searches on those computers to specific websites generating more than $14 million in fraudulent advertising fees for the cyber criminals.

The number of potential threats is expanding rapidly. A recent Cisco Systems study found that there were an estimated 12.5 billion electronic devices capable of connecting to the Internet in 2010. This number will increase to approximately 25 billion in 2015 and an astounding 50 billion by 2020. Given this continued expansion of computer communications networks, organizations such as NASA will face a digital battlefield of constantly evolving points of attack and new efforts to exploit weaknesses.

The challenge in successfully addressing cyber-security issues is particularly difficult at NASA. NASA owns a little less than half of the U.S. government's non-Defense web-sites. There are approximately 3,400 NASA controlled web-sites and nearly 1,600 of these are linked to the outside world. There are an estimated 176,000 individual IP addresses assigned to NASA's IT systems and networks. NASA also possesses more than 120,000 computer or related devices located at its centers and facilities that are connected to the Agency's IT networks. This huge system of nodes and networks presents enormous IT security challenges and potential IT vulnerabilities to the Agency. Over the past two years NASA reported more than 5,400 computer security intrusions that resulted in the installation of malicious software or unauthorized access to NASA's computer systems.

These cyber threats pose unique safety and security concerns to NASA. NASA's IT systems control spacecraft, including the Hubble Space Telescope and International Space Station, collect and process scientific data, contain records on a wide-array of technologically sophisticated intellectual property. These are all attractive targets for cyber-attack. Yet NASA cannot just take their systems off the internet to make them secure because they connect its thousands of scientists, engineers and other employees around the country to each other and connect NASA's human and information resources to the rest of the world.

Unfortunately NASA has a poor history of addressing cybersecurity threats. Insufficient efforts have been made in the past to take appropriate actions to confront and correct internal agency deficiencies. For example, the IG has re-investigated cyber-related issues it had identified in prior reports only to find the original weaknesses still uncorrected. These failures over time have exacerbated the agency's vulnerabilities. They certainly complicate efforts by the new leadership at NASA to address cybersecurity quickly and effectively.

NASA's IG has found that the Agency does not have an IT security configuration baseline across the agency. In other words, it is unclear what NASA's IT security is supposed to look like because there is no diagram of what it does look like. In addition, the IG has found that the Agency's vulnerability management practices have drastically underestimated the cyber-security threats and vulnerabilities NASA faces. And the Agency lacks a complete up-to-date inventory of all of its IT components.

Clearly it is easier to protect your home from a potential intruder if you know how many doors you have and where they are located. NASA does not appear to possess an accurate blueprint of its own house's IT infrastructure. Without that NASA cannot ensure that every potential gateway into the Agency is monitored and effectively protected.

My comments are not specifically directed at NASA's Office of the Chief Information Officer or Ms. Cureton, NASA's Chief Information Officer (CIO) who is testifying before us today. In fact, I hope my statement makes clear that I believe the problems with cybersecurity at NASA are many years in the making, and Ms. Cureton has had limited time to set things right. I am also aware that the CIO at NASA has limited authority to impose cybersecurity solutions across the entire NASA enterprise of contractors, Centers, and Mission Directorates. There seems to be a gap between the scope of your responsibility and the scope of your authority.

NASA's IT vulnerabilities must be identified and closed. Speed is critical in this context. If there are institutional or financial stumbling blocks that stand in the way of completing these critical tasks then I hope our witnesses will provide constructive suggestions to address them. The Committee is prepared to work with NASA to help close these gaps.

I believe this is an important subject and I look forward to hearing from our witnesses. Thank you Mr. Chairman.