Statement of Gil Vega

Associate Chief Information Officer for Cybersecurity and Chief Information Security Officer

U.S. Department of Energy

Before the

Subcommittee on Oversight and Investigations

Committee on Energy and Commerce

U.S. House of Representatives

March 27, 2012

Good morning Mr. Chairman Stearns and Members of the Subcommittee. I am pleased to testify on the Department of Energy's activities related to IT supply chain security. Thank you for this opportunity to testify today on the Government Accountability Office's (GAO) report titled *IT Supply Chain- National Security Related Agencies Need to Better Address Risk*s. The Department of Energy (DOE) appreciates the work performed by the GAO to identify opportunities to improve mission effectiveness and fiscal efficiency by reducing information technology (IT) supply chain risks. The DOE shares GAO's concern for these risks, which not only impact DOE's missions, but those of all federal agencies and the private sector in general. The DOE actively supports the goals outlined in the Administration's *National Strategy for Global Supply Chain Security* (January 2012) and by leveraging the collective, exceptional talent of the people in the DOE, we are committed to addressing these and other cybersecurity challenges.

Background

In November 2010, the GAO began a multi-agency review to identify efforts the Departments of Defense (DoD), Homeland Security (DHS), Justice (DOJ) and Energy (DOE) were taking to address IT supply chain risks. In response to its conclusions that agencies needed to better address supply chain risks, GAO's report directed three recommendations to DOE:

- Develop and document Departmental policy that defines which security measures should be employed to protect against supply chain threats;
- Develop, document and disseminate procedures to implement the supply chain protection security measures defined in departmental policy; and
- Develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain measures.

Department of Energy Response

It is clear that IT supply chain vulnerabilities threaten the missions of DOE and other federal agencies. As the Associate Chief Information Officer for Cybersecurity and the DOE Chief Information Security Officer, one of my roles is to understand and evaluate the cybersecurity threats to our missions and establish effective agency-wide programs to mitigate the associated risks in a cost-effective manner. Throughout my career, I have led similar efforts to effectively, and cost-efficiently, manage security risk.

In my short time at the DOE, I have been privileged to work with cybersecurity thought leaders in our National Laboratories and with interagency partners who are committed to addressing this national-level challenge by partnering and sharing information and best practices with each other, academia and industry. Aligned with the DOE Secretary’s goals related to energy, economic and national security, we are leveraging the experience and expertise of our National Laboratories to develop processes and technology to effectively secure DOE’s IT assets and information, and to protect the nation’s critical infrastructure.

Over the past 12 months, the DOE has been successful in developing and delivering several key foundational elements to properly address the broader cybersecurity threats we face every day, while strengthening our ability to meet the wide range of mission goals, which span open science to nuclear security. Among these accomplishments:

- DOE has developed and is implementing an agency-wide NIST-based Risk Management Approach with strategic direction and oversight by an Undersecretary-level Information Management Governance Council (IMGC). This raises corporate threat analysis and risk decision-making to senior management levels of the DOE and serves as a corporate foundation for managing our mission and investments with acceptable levels of risk. This is critical to the success and return on investment of current and future IT supply chain risk mitigation strategies.
- Under the direction and leadership of the IMGC, DOE is implementing an agency-wide Joint Cybersecurity Coordination Center, which will create a new cyber operational ecosystem with consolidated monitoring and reporting, collaborative information sharing and analysis, and coordinated incident response capabilities across the DOE. This is

critical to the effective monitoring of mitigation strategies implemented to address advanced cyber threats in general, and IT supply chain risks specifically.

As I previously stated, the DOE concurs with the GAO's recommendations. We are already addressing these in a coordinated manner by:

- Actively participating in the national-level policy discussions on Supply Chain Risk Management;
- Developing a supply chain cybersecurity strategy and policy that will foster DOE's interagency relationships and support the unified approach described in the Administration's *National Strategy For Global Supply Chain Security*;
- Developing a plan to implement the requirements of the recently released Committee on National Security Systems Directive 505, *Supply Chain Risk Management Directive for National Security Systems*;
- Working closely with the National Counterintelligence Executive and the broader National Intelligence and National Security communities to stay abreast of and counter new and growing threats to the nation's IT infrastructure; and
- Partnering with DHS and DoD, industrial control system manufacturers and energy critical infrastructure operators to identify and mitigate risks to industrial control systems.

While securing the supply chain will require more than any one agency can accomplish on its own, it is important to recognize the importance of the role played by DOE's National Laboratories, which have been at the forefront of identifying and mitigating vulnerabilities in the IT supply chain. The DOE National Laboratories have developed and are actively improving capabilities in software and hardware assurance to mitigate risks, particularly to our National

Security Systems and to the safety, security and reliability of the nuclear weapons stockpile. The DOE works closely with DoD, DHS, the National Security Agency, the Department of Commerce, and the General Services Administration on these emerging capabilities.

Conclusion

In conclusion, the GAO report has identified areas of needed improvement for IT supply chain security at the DOE and we concur with the report's recommendations. We believe GAO understands the national challenge IT supply chain risks pose to all federal agencies as well as the private sector and believe further congressional support for a nationally coordinated response is required.

The DOE strongly supports the goals of the *National Strategy for Global Supply Chain Security*, which address the need to "promote the secure and efficient movement of goods" and to "foster a resilient supply chain". To this end, the Administration has communicated that it seeks to align Federal activities across the United States Government, including in our partnerships with industry. The DOE believes that this unified approach is the right approach, and that policies and standards to address IT supply chain risk management must be coordinated at the national level, not developed independently through individual agencies.

Meanwhile, at DOE, we understand how important our role is as the sector-specific agency, as designated under Homeland Security Presidential Directive-7, for the nation's energy critical infrastructure and as a cornerstone of our nuclear security. We will continue our efforts to strengthen cybersecurity in these specific programs, as well as across the entire DOE enterprise.

Thank you for this opportunity to discuss the report’s findings. Mr. Chairman, this concludes my statement and I look forward to answering your questions.