STATEMENT OF

KEVIN CHAREST

CHIEF INFORMATION SECURITY OFFICER,

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

ON

HEALTHCARE.GOV

BEFORE THE

U. S. HOUSE COMMITTEE ON OVERSIGHT & GOVERNMENT REFORM

JANUARY 16, 2014

U. S. House Committee on Oversight and Government Reform

January 16, 2014

Good morning Chairman Issa, Ranking Member Cummings, and Members of this Committee. My name is Kevin Charest and I am the Chief Information Security Officer for the U.S. Department of Health and Human Services (HHS or Department).

The Department of Health and Human Services (HHS) is the United States Government's principal agency for protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves. The HHS Office of the Secretary (OS) and the Department's eleven Operating Divisions administer more than 300 programs, covering a wide spectrum of activities. HHS's Operating Divisions include: the Administration for Children and Families, the Administration for Community Living, the Agency for Healthcare Research and Quality, the Agency for Toxic Substances and Disease Registry, the Centers for Medicare & Medicaid Services (CMS), the Centers for Disease Control and Prevention, the Food and Drug Administration, the Health Resources and Services Administration, the Indian Health Service, the National Institutes of Health, and the Substance Abuse and Mental Health Services Administration.

The Office of the Chief Information Officer (OCIO), in which I serve, is a part of OS. Our responsibility, as one of the Staff Divisions of OS, is to manage programs within OS and support the eleven Operating Divisions in carrying out their various and diverse missions. It is important to point out, however, that we manage the Department's information technology (IT) portfolio

through a federated governance structure. The vast majority of the Department's IT resources are tied directly to the appropriations and statutory authorities Congress provides directly to our programs and Operating Divisions. Our governance authorities at the OS level reflect that federated structure. Thus, many of HHS's Operating Divisions have their own Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and IT management structure – the exception to this rule is in OS where the Department CIO and CISO perform those responsibilities.

My office convenes and leads the HHS Chief Information Security Officer Council, through which we and Operating Divisions' CISOs discuss and collaboratively develop Department-wide policies and share best practices and common tools involving IT security. However, program-level IT decisions, including those involving IT security, are made by our Operating Divisions at the Operating Division level, as in the instance of HealthCare.gov, the topic of today's hearing. As the "business owner" of HealthCare.gov, as is the case with Medicare.gov, CMS is responsible for IT security for the website. To date, there have been no successful security attacks on Healthcare.gov and no person or group has maliciously accessed personally-identifiable information (PII) from the site.

HHS' enterprise-wide information security and privacy program was launched in fiscal year 2003 to help protect HHS, including its Operating Divisions, against potential information technology (IT) threats and vulnerabilities. The Program ensures compliance with Federal mandates and legislation, including the Federal Information Security Management Act (FISMA). Under my leadership, I have established a framework for Operating Divisions to regularly report

incidents involving IT Security to my office. Operating Divisions routinely report potentia1 information security incidents to the HHS Computer Security Incident Response Center (CSIRC), which I oversee.

Proactively identifying and addressing security "incidents" is a regular part of the process we require all Operating Divisions to employ. Security incidents include attacks and activities that may violate security policies, such as changes to system hardware without permission, the unauthorized use of hardware for accessing data, and attempts—either failed or successful—to gain unauthorized access to a system. A breach of PII may occur as a result of a security incident.

Often, upon further investigation, these security incidents turn out to be false positives. However, out of an abundance of caution, we investigate all such incidents to understand what actually occurred, and when necessary to develop an appropriate risk mitigation strategy to minimize future such incidents.

In addition to our internal investigation of all IT security incidents, we report all such incidents to the Department of Homeland Security's (DHS) Computer Emergency Readiness Team (US-CERT), at DHS' National Cybersecurity and Communications Integration Center. Through US-CERT's operations center, US-CERT accepts, triages, and collaboratively responds to incidents; provides technical assistance to information system operators; and disseminates timely notifications regarding current and potential security threats and vulnerabilities. For reference, in

fiscal year 2013, US-CERT processed approximately 228,700 cyber incidents, an average of more than 620 per day, involving Federal Agencies, critical infrastructure, and industry partners. It is important to note that HHS operates a defense–in-depth strategy for protecting its IT assets in accordance with guidance issued by the Office of Management and Budget and the National Institute of Standards and Technology, which has been reflected in HHS's information security policy. This strategy includes the use of a risk based approach to authorizing systems to operate, a robust set of technologies for continuous monitoring of systems, standards and minimum requirements for systems, as well as appropriate business processes and controls to ensure the confidentiality, integrity, and availability of all HHS IT assets in operation. In addition, HHS promptly notifies individuals of breaches that could compromise their protected information, when warranted.

Consistent with these policies, CMS reports actual or suspected computer-security incidents in connection with HealthCare.gov to the CSIRC. The reports are based on the operational security protections CMS has in place to deter and prevent unauthorized access, and weekly penetration testing and security scans of the system. CMS's Chief Information Security Officer (CISO) and its Information System Security Officer (ISSO) are responsible for designing and maintaining a security program to mitigate any risks identified, in accordance with FISMA.

In all cases, HHS takes mitigation of any IT security incidents, particularly those involving a PII breach, seriously and reviews Operating Division incident reports to ensure that mitigation solutions are applied appropriately and expediently. The process of determining risk and response begins immediately upon discovery of an incident:

- Employees are required to report any suspected or confirmed privacy incidents to each Agency's Incident Response Team or the HHS CSIRC as expeditiously as possible.
- The HHS CSIRC is required to report incidents involving PII within one hour to US-CERT.

Additionally, building on Federal guidelines and regulations, and in conformance with industry standards, HHS has dedicated teams of career experts, including officials from the Office of the Chief Information Officer, the Office of Inspector General, the Office for Civil Rights' Privacy Office, the CSIRC and key Operating Divisions, who work around the clock to identify, manage, and mitigate suspected or potential breaches of PII.

In carrying out their work, these teams abide by HHS's PII Breach Response Team Policy, published in 2008, and HHS's Privacy Incident Response (PIRT) Charter, published in 2011. HHS security and privacy experts work with appropriate Federal Government and industry professionals to:

- Validate risk and review and approve response plans;
- Review and approve communications or notice to affected individuals;
- Perform analysis on data in order to recommend strategies to effectively refine and improve the Department's response to the potential loss of PII;
- Implement privacy and security solutions that can reduce the potential loss of PII; and
- Monitor the privacy and security environment to raise awareness of threats to PII within the Department.

If the team determines that notification of a breach is warranted, the Operating Division coordinates through the PIRT to send letters to the affected consumers or businesses, informing them of the breach.

I appreciate the opportunity to meet with you today, and to discuss your interest in the Federal Government's IT security practices.