CSIS Report		**60 Day Review**
1. Create a comprehensive national security strategy for cyberspace.	☑	Calls for an updated national strategy to secure the information and communications infrastructure.
2. Publish a public doctrine for protection and deterrence.	☑	In his May 29 speech, the President declared that “From now on, our digital infrastructure, the networks and computers we depend on every day, will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect and defend against attacks, and recover quickly from any disruptions or damage.”
3. Open the discussion of the issues of deterrence and strategy in cyberspace to a broad national community of experts and stakeholders.	☑	The review itself was remarkably transparent and involved extensive consultations with private sector groups
Organizing for Cybersecurity		
4. the President should appoint an Assistant for Cyberspace and establish a cyberspace directorate in the NSC that absorbs existing HSC functions.	☑	Not an Assistant, but a cyber advisor; level to be determined whom the President said in his May 29 speech will have direct access. NSC cyber directorate absorbs functions of the HSC
5. The work of the Assistant for Cyberspace and the new NSC directorate would be supported by a new EOP office – the National Office for Cyberspace.	☠	No new office.
6. Existing agencies would keep responsibility for their current operational activities, under the oversight of the NSC and the new EOP Cyberspace office	☑	White House to coordinate policy and agency implementation.
7. OMB would maintain oversight of the budget functions, in coordination (as it does for other policy areas) with the NOC and the NSC.	☑	The new advisor will “ensure that the President’s budget reflects federal priorities for cybersecurity, and develop a legislative agenda, all in consultation with the Federal government’s Chief Technology Officer and Chief Information Officer—along with the appropriate entities within the Office of Management and Budget (OMB)” and a host of other White House entities.
Private Sector Partnerships		
8. We recommend the President direct the creation of new groups for partnership that put trust and action	☠	A general commitment to rebuilding public private partnership.

at their core, not information sharing:		
Regulate Cyberspace		
9. The President should task the NOC to work with appropriate agencies, to develop and issue standards and guidance for securing critical cyber infrastructure those agencies would then apply in their own regulations.	☑	The US should consider options including “adjustments to liability considerations (reduced liability in exchange for improved security or increased liability for the consequences of poor security), indemnification, tax incentives, and new regulatory requirements and compliance mechanisms.”
Industrial Control Systems		
10. The NOC should work with the appropriate regulatory agencies and with NIST to develop regulations for control systems.	☠	No mention of SCADA or Industrial Control Systems
11. The NOC should immediately determine the extent to which government-owned critical infrastructures are secure from cyber attack, and work with the appropriate agencies to secure these infrastructures.	☠	No tasking for assessing security of government infrastructure.
Use Acquisitions to Improve Security		
12. The President should direct the NOC and CIO Council, working with industry, to develop and implement security guidelines for the procurement of software products.	☑	“The government, working with State and local partners, should identify procurement strategies that will incentivize the market to make more secure products and services available to the public.”
13. The President should task NSA and NIST, working with international partners, to reform the NIAP process.	☑	No specific mention of the NIAP, but a general commitment to work with foreign partners on a range of issues, including standards
Purchase Secure Services		
14. The U.S. should develop mandatory requirements for agencies to contract only with telecommunications carriers that use secure internet protocols. As part of its larger international strategy, the U.S., in partnership with like-minded nations, would work for acceptance for global endorsement of the more secure protocols.	☠	No requirement to use secure protocols
Identity Management		

15. The United States should make strong authentication of identity, based on robust in-person proofing and thorough verification of devices, a mandatory requirement for critical cyber infrastructures (telecom, energy, finance, government services).	☑	"The Federal government—in collaboration with industry and the civil liberties and privacy communities—should build a cybersecurity-based identity management vision and strategy for the Nation that considers an array of approaches, including privacy-enhancing technologies."
16. The United States should allow consumers to use strong government-issued credentials (or commercially-issued credentials based on them) for online activities, consistent with protecting privacy and civil liberties.	☠	No discussion of consumer use, but recommendation to allow emergency responders and critical infrastructure operators to use federal credentials
17. In a related initiative, the FTC should implement regulations that protect consumers by preventing businesses and other services from requiring strong government-issued or commercially-issued credentials for all online activities.	☠	No discussion of consumer use
18. Finally, the President should require each agency to report on how many of their employees, contractors and grantees are using credentials that comply with HSPD 12, and restrict bonuses or awards at agencies which have not fully complied by January 2010.	☑	"The Federal government should ensure resources are available for full federal implementation of HSPD-12"
Modernize Authorities		
19. The President should direct the Department of Justice to work with Congress to update laws applying to criminal investigations of online crime (including espionage and terrorism).	☑	"The Federal government should identify any gaps in law enforcement capacity or investigative authority needed to defend the Nation's infrastructure. Any new authorities would need to be consistent with the protection of civil liberties and privacy rights."
20. The Attorney General should issue guidelines as to the circumstances and requirements for deciding when Titles 3 and 18 (law enforcement), Title 10 (military authorities) or Title 50 (intelligence) are appropriate.	☠	A general commitment to "convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses . . . and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government."

The Federal Information Security Management Act (FISMA)		
21. The President should work with Congress to rewrite FISMA to use performance-based measurements of security.	☑	"The Administration should work with Congress to update and strengthen this legislation."
Civilian and National Security Systems.		
The President should propose legislation that replaces the current security-civilian split with a risk-based approach. The NOC working with NIST and other agencies should develop a risk-based set of computer security policies that apply to all federal IT systems.	☑	"Responsibility for a federal cyber incident response is dispersed across many federal departments and agencies because of the existing legal, but artificial, distinctions between national security and other federal networks..... Any consolidation of authorities in a unified structure may require legislation."
Cyber Education and Workforce Development		
22. The President should direct the NOC to work with the relevant agencies and the Office of Personnel Management to create training programs and career paths for the federal cyber workforce, and to work with the National Science foundation to develop national education programs.	☑	"Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government" and "Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy."
Research and Development		
25. The NOC, working with OSTP, should provide overall coordination of cybersecurity R&D and to increase cybersecurity R&D resources.	☑	"In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies. "