Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C.

In the Matter of	)	
	)	
National Broadband Plan Recommendation	)	**PS Docket No. 10-146**
To Create A Cybersecurity Roadmap	)	
	)	
National Broadband Plan for Our Future	)	**GN Docket No. 09-51**
	)	

COMMENTS OF THE UNITED STATES TELECOM ASSOCIATION

Its Attorneys:

Jonathan Banks
Robert Mayer
Kevin Rupy
607 14th Street, NW
Suite 400
Washington, D.C. 20005
(202) 326-7300

September 23, 2010

Table of Contents

Summary ..... **iii**

I. GREATER COORDINATION OF FEDERAL CYBERSECURITY EFFORTS IS NEEDED FOR ALL FEDERAL AGENCY STAKEHOLDERS **2**

II. THE COMMISSION SHOULD CONTINUE TO ENGAGE IN EXISTING PUBLIC PRIVATE PARTNERSHIPS AND CYBERSECURITY OUTREACH EFFORTS. **4**

A. The Commission Should Continue to Participate in Existing Public Private Cybersecurity Coordination Efforts **4**

B. The Federal Government Should Engage in Cybersecurity Education and Awareness Efforts. **7**

III. THE DEPARTMENT OF HOMELAND SECURITY IS THE APPROPRIATE AGENCY FOR COORDINATING THE NATION'S CYBERSECURITY EFFORTS. **10**

IV. CONCLUSION. **12**

* * *

SUMMARY

There is urgent need for the federal government to ensure greater coordination at the federal level of governmental cybersecurity efforts. As a growing number of agencies move into the cybersecurity realm, there is an increasing level of redundant efforts and clouded authority. Such duplicative and inconsistent initiatives can often drain scare resources from substantive cybersecurity activity. This is not to say that the Commission or other agencies should refrain from engaging in cybersecurity issues. Rather, there needs to be one central point of coordination to direct the nation's singular cybersecurity policy.

USTelecom also urges the Commission to continue to engage in existing public private partnerships and cybersecurity outreach efforts. The Commission's increased involvement in the public private framework enables it to better contribute to enhanced protection, detection, mitigation and response to events that occur in the broad cybersecurity ecosystem. For example, USTelecom applauds the participation of Commission staff in developing the 2011 National Sector Risk Assessment that is being coordinated under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework. The nation's cybersecurity efforts are significantly enhanced by the Commission's leadership and expertise in the communications arena.

USTelecom also urges the Commission to promote public outreach in the area of cybersecurity. Whether implemented on a broad public relations scale, or through targeted industry working groups, such outreach measures ensure that valuable information is disseminated and shared amongst target audiences. The federal government has a long track record of tremendously successful outreach in other areas, and such an approach is ideally suited for informing consumers and small businesses about critical issues in the cybersecurity context.

Finally, USTelecom has noted the increasing problem in the cybersecurity domain of conflicting and uncoordinated roles by disparate agencies. As issues of cybersecurity continue to move to the forefront, it is increasingly imperative that the Commission – and other relevant agency stakeholders – follow existing and established legal precedent relating to cybersecurity roles and responsibilities. The Department of Homeland Security (DHS) is the designated lead agency on matters relating to cybersecurity. To better ensure the development of a clear strategy for securing the nation's communications networks, the Commission should assist DHS in developing such a strategy.

* * *

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C.

In the Matter of	)	
	)	
National Broadband Plan Recommendation	)	**PS Docket No. 10-146**
To Create A Cybersecurity Roadmap	)	
	)	
National Broadband Plan for Our Future	)	**GN Docket No. 09-51**
	)	

COMMENTS OF
THE UNITED STATES TELECOM ASSOCIATION

The United States Telecom Association (USTelecom)[1] is pleased to comment on the Notice of Inquiry (*Notice*)[2] issued by the Federal Communications Commission (Commission) in the above referenced proceeding. USTelecom agrees that there is a need for a "clear strategy for securing the vital communications networks,"[3] and it is imperative that such a strategy be established in a coordinated and rational manner. The government entity best able to lead development and implementation of this strategy is the Department of Homeland Security (DHS), the designated central agency in cybersecurity issues. The Commission should therefore coordinate any of its cybersecurity efforts with DHS. USTelecom is encouraged that the Commission continues to participate in cybersecurity efforts through ongoing public private

---

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data and video over wireline and wireless networks.

[2] Public Notice, *FCC Seeks Comment on National Broadband Plan Recommendation to Create a Cybersecurity Roadmap*, DA-10-1354 (August 9, 2010) (*Notice*).

[3] *Notice*, p. 1 (citing Omnibus Broadband Initiative, Federal Communications Commission, *Connecting America: The National Broadband Plan* (March 2010) at 123 (Recommendation § 16.5)).

partnerships. Such public private efforts can be further enhanced through government agencies' public awareness outreach on matters relating to cybersecurity.

I. GREATER COORDINATION OF FEDERAL CYBERSECURITY EFFORTS IS NEEDED FOR ALL FEDERAL AGENCY STAKEHOLDERS.

The wide range of uncoordinated and sometimes conflicting federal government cybersecurity initiatives – including the Commission's efforts to establish a Cybersecurity roadmap – highlight the importance of the need for the federal government to ensure greater coordination at the federal level of governmental cybersecurity efforts. Indeed, commenters in this proceeding have already appraised the Commission of this critical need.

For example, Qwest emphasized the need for "Federal agency coordination in effectuating Federal government cyber security policy."[4] Similarly, Verizon stressed the "importance of the Federal Government centralizing and clarifying government roles and responsibilities," and correctly points out that such clarification prevents "duplicative or inconsistent initiatives that could drain scare resources from substantive cybersecurity activity."[5]

Both commenters stress the urgent need for greater coordination at the federal level over the increasing number of federal agencies becoming involved with cybersecurity issues. As these growing number of agencies move into the cybersecurity realm, there is an increasing level of redundant efforts and clouded authority. For example, a search for the word "cybersecurity" on the federal government website "Regulations.gov" yields 23 separate dockets since January

---

[4] Qwest Ex Parte, August 19, 2010, PS Docket No. 10-146, GN Docket No. 09-51.

[5] Verizon Ex Parte, September 14, 2010, PS Docket No. 10-146, GN Docket No. 09-51.

2010, while a search for "cyber security" yields 73 dockets (see Attachment A). These proceedings have been initiated by a broad range of federal entities, including, for example, the Department of Homeland Security, the Department of Energy, the National Science Foundation the Department of Agriculture, and the White House.

Moreover, these search results do *not* include additional, certain proceedings that have in fact been initiated by federal agencies, thereby further confusing relevant stakeholders in these proceedings. Of particular note, this very proceeding initiated by the Commission does not show up in the Regulations.gov list of open dockets.[6]

This is not to say that the Commission or other agencies should refrain from engaging in cybersecurity issues. Rather, there needs to be one central point of coordination to direct the nation's singular cybersecurity policy. As one witness before the House Subcommittee on House Committee on Homeland Security, Sub-Committee on Emerging Threats, Cybersecurity, and Science and Technology, testified last year, "[t]he sheer number of extremely important issues that transcend agency boundaries suggests that the coordination of any national cybersecurity strategy must reside within the one organization responsible for ensuring that the government acts as one government."[7]

---

[6] USTelecom conducted a search of the Federal government website "regulations.gov" on September 14, 2010. Although the *Notice* was released on August 9, 2010, it does not appear in search results attached to these comments as Attachment A.

[7] Written Testimony of Scott Charney, Corporate Vice President, Microsoft Corporation's Trustworthy Computing, Securing America's Cyber Future: Simplify, Organize and Act, Before the House Committee on Homeland Security, Sub-Committee on Emerging Threats, Cybersecurity, and Science and Technology, Hearing on Reviewing the Federal Cybersecurity Mission, March 10, 2009.

II. THE COMMISSION SHOULD CONTINUE TO ENGAGE IN EXISTING PUBLIC PRIVATE PARTNERSHIPS AND CYBERSECURITY OUTREACH EFFORTS.

In previous proceedings regarding cybersecurity issues, USTelecom has expressed strong support for the existing public-private mechanisms and governmental public awareness campaign efforts. These proven approaches can have a tangible and positive impact on the nation's cybersecurity, and have been identified by the White House as part of its near term action plan.[8]

A. The Commission Should Continue to Participate in Existing Public Private Cybersecurity Coordination Efforts

USTelecom has commented at length about the increasingly robust public-private mechanism that is addressing cyber incident management and coordination.[9] These joint efforts are designed to address both strategic and operational aspects of cybersecurity policy and risk management.

USTelecom is encouraged that the Commission has become increasingly engaged in the existing public private cybersecurity framework. Through such involvement, the Commission can better contribute to enhanced protection, detection, mitigation and response to events that occur in the broad cybersecurity ecosystem. Such involvement demonstrates the Commission's recent acknowledgement that its proper role in the cybersecurity realm "is to complement and

---

[8] *See White House Cyberspace Policy Review*, p. 37 (identifying as a near term action plan the initiation of a national public awareness and education campaign to promote cybersecurity).

[9] *See e.g.*, Comments of USTelecom at the FCC, *Cyber Security Certification Program*, pp. 7 – 17, PS Docket No. 10-93 (submitted July 12, 2010) (*USTelecom Cyber Certification Comments*).

support efforts by the Justice and Homeland Security departments."[10] The importance of interagency coordination in implementing cybersecurity initiatives also was recently identified by The White House as a key component to the nation's cybersecurity action plan.[11]

In this regard, USTelecom applauds the participation of FCC staff in developing the 2011 National Sector Risk Assessment that is being coordinated under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework.[12] As a member of the Government Communications Coordinating Council (GCCC), the FCC will be working with representatives from the wireline, wireless, satellite, cable and broadcasting industries through their membership in the Communications Sector Coordinating Council (CSCC).

The FCC, other federal agencies, and industry experts will examine threats, risks and vulnerabilities to the communications sector associated with physical, cyber, and human factor elements. This is a major undertaking and project leadership includes representatives from the Department of Agriculture, the Department of Defense, and the Department of Homeland Security. USTelecom believes that the FCC brings critical capabilities and perspectives to this

---

[10] Adam Bender, *FCC Aims to Do More on Cybersecurity*, Communications Daily, November 3, 2009 (noting a statement by Public Safety & Homeland Security Bureau spokesman Robert Kenny that the Commission believes its role is to complement and support efforts by the Justice and Homeland Security departments.).

[11] *See White House Cyberspace Policy Review*, p. 37 (identifying as a near term action plan the convening of appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulating coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government).

[12] *See* DHS Website, Critical Infrastructure Partnership Advisory Council (available at: http://www.dhs.gov/files/committees/editorial_0843.shtm) (visited September 22, 2010).

effort, FCC engagement enhances the viability of the public-private partnership model that many in government and industry have described as essential, especially in the arena of Cybersecurity.[13]

The FCC should seek to build upon this work by pursuing further opportunities for engagement with other government entities working on cybersecurity initiatives. The Commission should consider greater collaboration with existing government cybersecurity related entities including the National Science Foundation and the National Institute of Standards and Technology (NIST)[14] Computer Security Division as well as coordination during cyber incident response with the U.S. CERT. The Commission could strengthen its visibility in the

---

[13] President Obama emphatically framed his Administration's cybersecurity policy when he stated, "[s]o let me be very clear: My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity." *See*, Speech of President Barack Obama, *Remarks By The President On Securing Our Nation's Cyber Infrastructure*, May 29, 2009 (available at: http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/) (visited September 22, 2010); *see also*, DHS Secretary's Web Address on Cybersecurity, *A New Challenge for Our Age: Securing America Against the Threat of Cyber Attack*, October 20, 2009 (available at: http://www.dhs.gov/ynews/gallery/gc_1256070988236.shtm) (visited September 22, 2010).

[14] The Computer Security Division (CSD), a component of NIST's Information Technology Laboratory (ITL), provides standards and technology to protect information systems. The CSD is a source for substantial expertise related to certifications and accreditations. NIST is currently engaged in various activities that are consistent with areas of expertise inherent in the Commission's ongoing activities. This includes NIST's Smart Grid Interoperability Project, as well as projects relating to cybersecurity. *See e.g.*, NIST Press Release, *Commerce Secretary Unveils Plan for Smart Grid Interoperability*, released September 24, 2009 (available at: http://www.nist.gov/public_affairs/releases/smartgrid_092409.cfm) (visited July 7, 2010); *see also*, NIST Press Release, *NIST Releases Final Version of New Cybersecurity Recommendations for Government*, released July 31, 2009 (available at: http://www.nist.gov/public_affairs/techbeat/tbx2009_0731_sp800-53iii.htm) (visited July 7, 2010).

recently established National Cybersecurity and Communications Integration Center (NCCIC), which brings together various government organizations responsible for protecting cyber networks and infrastructure and private sector partners.[15] The value of these organizations and efforts will be significantly enhanced by the Commission's leadership and expertise in the communications arena.

B. The Federal Government Should Engage in Cybersecurity Education and Awareness Efforts.

In previous proceedings regarding cybersecurity issues, USTelecom has expressed strong support for governmental outreach efforts.[16] Such an approach can have a tangible and positive impact on the nation's cybersecurity, and was previously identified by the White House as part of its near term action plan.[17] The Commission, in particular, should consider government outreach to discrete areas in the cybersecurity environment, specifically the consumer and small business communities to ensure implementation of effective cybersecurity practices.

Public outreach measures have been successfully implemented by the federal government in the past and are ideally suited in the current context. Whether implemented on a broad public

---

[15] *See e.g.*, DHS Press Release, *Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center*, October 30, 2009 (available at: http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm) (visited September 21, 2010) (*NCCIC Press Release*).

[16] Comments of USTelecom at the FCC, *Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan, NBP Public Notice # 8*, pp. 17 – 19, GN Docket Nos. 09-47, 09-51, 09-137 (submitted November 12, 2009).

[17] *See White House Cyberspace Policy Review*, p. 37 (identifying as a near term action plan the initiation of a national public awareness and education campaign to promote cybersecurity).

relations scale, or through targeted industry working groups, such outreach measures ensure that valuable information is disseminated and shared amongst target audiences.

For example, in the industry working group context, the Commission recently renewed the charter for the Communications Security, Reliability, and Interoperability Council (CSRIC).[18] The purpose of the CSRIC is to provide recommendations to the Commission to ensure optimal security, reliability, operability and interoperability of communications systems, including public safety, telecommunications, and media communications systems.

In order to further maximize its efforts, the Commission also established Working Group 2A of the CSRIC (Cybersecurity Best Practices). Working Group 2A is currently examining cybersecurity best practices, including those pertaining to all segments of the communications industry and public safety communities.[19] These ongoing public-private efforts are generating noticeable results that will further the efforts of industry and government to identify and prioritize the most critical best practices for communications providers to adopt and implement.

Further outreach, particularly to the consumer and small business communities, can be coordinated through broader federal government public policy campaigns. The federal government has a long track record of tremendously successful outreach in other areas, and such

---

[18] *See*, Public Notice, *FCC Seeks Nominations by May 11, 2009 for Membership on the Communications Security, Reliability, and Interoperability Council (CSRIC)*, DA 09-816, 24 FCC Rcd 4201 (2009).

[19] *See*, CSRIC website, *CSRIC Working Group Descriptions, Working Group 2A – Cybersecurity Best Practice* (available at: http://www.fcc.gov/pshs/advisory/csric/wg-2a.pdf) (visited September 21, 2010).

an approach is ideally suited for informing consumers and small businesses about critical issues in the cybersecurity context.[20]

The Ad Council has highlighted the success of many of its public awareness campaigns, noting that results of its campaigns have made "lasting and positive social change."[21] Among other highlights, it notes that the Department of Homeland Security's Ready.gov website received over 18 million unique visitors within the first ten months of the launch of the preparedness campaign.

The impact of government campaigns can be seen across a wide variety of issue areas. Forests destroyed by wildfires decreased substantially – from 22 million acres to less than 8.4 million acres per year -- since the Forest Fire Prevention campaign began. After the launch of the Environmental Defense campaign, the amount of total waste recycled in 2000 increased by 24.4% as compared to 1995, and 385.4% as compared to the 1980s . In addition, safety belt usage has increased from 14% to 79% since the Safety Belt campaign launched in 1985 -- a change that is estimated to have saved 85,000 lives, and $3.2 billion in costs to society.[22]

In the cybersecurity context, the federal government could focus on raising consumer and business awareness on issues relating to cybersecurity. Such outreach could emphasize

---

[20] The CGB has conducted extensive outreach in several critical areas, including the Rural Health Care Pilot Program, Lifeline and Link-Up, the Do-Not-Call Registry and the digital television transition (*see* CGB website, available at: http://www.fcc.gov/cgb/ (visited July 7, 2010).

[21] Ad Council website (available at: http://www.adcouncil.org/default.aspx?id=68) (visited September 8, 2010).

[22] Ad Council website (available at: http://www.adcouncil.org/default.aspx?id=68) (visited September 8, 2010).

individual responsibility as critical tool for defeating cyber-attackers, or focus on such issues as digital hygiene (*e.g.*, emphasizing the importance of not sharing user identification names or passwords, password protecting important documents, etc.). One such approach targeted towards children and parents was announced by the FCC earlier this year.[23]

III. THE DEPARTMENT OF HOMELAND SECURITY IS THE APPROPRIATE AGENCY FOR COORDINATING THE NATION'S CYBERSECURITY EFFORTS.

The Department of Homeland Security (DHS) is the designated lead agency on matters relating to cybersecurity. As USTelecom has noted, an increasing problem in the cybersecurity domain is the presence of conflicting and uncoordinated roles by disparate agencies in the cybersecurity venue. As issues of cybersecurity continue to move to the forefront, it is increasingly imperative that the Commission – and other relevant agency stakeholders – follow existing and established legal precedent relating to cybersecurity leadership roles and responsibilities.

In this regard, DHS's authority over cybersecurity issues arises from the issuance of a Homeland Security Presidential Directive (HSPD) in 2003.[24] The legal guidance contained in HSPD-7 is unequivocal: DHS is responsible "for coordinating the nation's overall critical

---

[23] Prepared Remarks of Chairman Julius Genachowski, Federal Communications Commission, Digital Opportunity: A Broadband Plan for Children and Families, National Museum of American History, Washington, D.C., March 12, 2010 (available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-296829A1.pdf) (visited July 10, 2010).

[24] HSPDs are a form of executive order issued by the President of the United States. Many HSPDs address matters of critical infrastructure, including those relating to telecommunications.

infrastructure protection efforts, including for cyber infrastructure."[25] Moreover, while HSPD-7 acknowledges that "each infrastructure sector possesses its own unique characteristics and operating models,"[26] the Commission is not designated as one of the "Sector-Specific agencies" with specific authority to "conduct or facilitate vulnerability assessments" of an assigned sector.[27]

HSPD-7 assigned the Secretary of DHS with the responsibility "for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States."[28] HSPD-7 further directs all Federal departments and agencies to both "coordinate and cooperate with the [DHS]" in order to protect critical infrastructure and key resources.[29] Although the directive broadly addresses *all* forms of critical infrastructure, in assigning responsibility for those relating to cybersecurity HSPD-7 is explicit. It states that DHS is to maintain an organization that will "serve as focal point for the security of cyberspace."[30]

---

[25] *See* White House Report, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 29, 2009, p. 4 (*White House Cyberspace Policy Review*).

[26] Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, ¶ 18 (available at: http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm) (visited September 21, 2010) (*HSPD-7*).

[27] *HSPD-7*, ¶19(a).

[28] *Id.*, ¶12.

[29] *Id.*, ¶23.

[30] *HSPD-7*, ¶16.

In this regard, the National Cyber Security Division (NCSD) is DHS's lead agency for securing cyberspace and the nation's cyber assets and networks.[31] The NCSD is fulfilling its mandate contained in HSPD-7 by working collaboratively with public, private and international entities to secure cyberspace and the nation's cyber assets.

USTelecom shares the Commission's view that "[t]he country needs a clear strategy for securing the vital communications networks upon which critical infrastructure and public safety communications rely."[32] To better ensure the development of a clear strategy for securing the nation's communications networks, the Commission should assist DHS in developing such a strategy.

IV. CONCLUSION.

USTelecom strongly supports ongoing efforts to secure the nation's critical communications from cybersecurity vulnerabilities. In order to achieve this goal, there is a need for greater coordination at the federal level of governmental cybersecurity efforts. While the Commission has an important role to fulfill in this arena, it should not usurp the authority of the DHS in matters of cybersecurity. Rather, the Commission should complement cybersecurity efforts through active participation in the existing public private partnership, and through increased public awareness campaigns on cybersecurity issues.

---

[31] See DHS website, *National Cyber Security Division*, (available at: http://www.dhs.gov/xabout/structure/editorial_0839.shtm) (visited September 15, 2010).

[32] *Notice*, p. 1.

Respectfully submitted,

UNITED STATES TELECOM ASSOCIATION

By: _____

Jonathan Banks
Robert Mayer
Kevin Rupy

607 14th Street, NW, Suite 400
Washington, D.C. 20005

Attachment A

Search Results

New Search Search Within Results Search Advanced Search

Too many results? Narrow them here:

Agency

Find Agency:

- DHS (8)
- DOE (2)
- FCC (1)
- FDA (1)

Document Type

- Public Submissions (17)
- Other (0)
- Supporting & Related Materials (3)
- Notices
- Rules
- Proposed Rules

Docket Type

- Rulemaking (4)
- Nonrulemaking (14)

Comment Period

- Open (1)
- Closed (28)

Comment Period

From: MM/DD/YY

To: MM/DD/YY

Posted Date

From: 01/01/10

To: 09/14/10

29 results for "cybersecurity"

Records Per Page: 50

View By Relevance | View By Docket Folder

Title	Document Type	ID	Actions
Office of the Secretary; Published Privacy Impact Assessments on the Web (1 Document)	Docket Folder	DHS-2009-0029	Open Docket Folder Sign up for Email Alert
National Protection and Programs Directorate; Statewide Communication Interoperability Plan Implementation Report (1 Document)	Docket Folder	DHS-2010-0002	Open Docket Folder Sign up for Email Alert
New Information Collection Request, Communications Unit Leader (COML) Prerequisite and Evaluation (1 Document)	Docket Folder	DHS-2010-0004	Open Docket Folder Sign up for Email Alert
New Information Collection Request, Technical Assistance Request and Evaluation (1 Document)	Docket Folder	DHS-2010-0006	Open Docket Folder Sign up for Email Alert
New Information Collection Request, Sector-Specific Agency Executive Management Office Meeting Registration (1 Document)	Docket Folder	DHS-2010-0019	Open Docket Folder Sign up for Email Alert
New Information Collection Request, Statewide Communication Interoperability Plan Implementation Report (1 Document)	Docket Folder	DHS-2010-0021	Open Docket Folder Sign up for Email Alert
Agency Information Collection Activities: Submission for Review; Information Collection Request for the Department of Homeland Security (DHS) Science and Technology Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT) program - 60-day Notice (1 Document)	Docket Folder	DHS-2010-0043	Open Docket Folder Sign up for Email Alert
PREDICT (1 Document)	Docket Folder	DHS-2010-0073	Open Docket Folder Sign up for Email Alert
This docket contains Federal Register Notices from the DOE FDMS Sandbox. (1 Document)	Docket Folder	DOE-HQ-2009-0003	Open Docket Folder Sign up for Email Alert
Implementing the National Broadband Plan (1 Document)	Docket Folder	DOE-HQ-2010-0012	Open Docket Folder Sign up for Email Alert
Framework for Broadband Internet Service (1 Document)	Docket Folder	FCC-2010-0184	Open Docket Folder Sign up for Email Alert

Comprehensive List of Current Guidance Documents at FDA (1 Document)	Docket Folder	FDA-1998-N-0050	Open Docket Folder Sign up for Email Alert
Transmission Relay Loadability Reliability Standard (1 Document)	Docket Folder	FERC-2009-0781	Open Docket Folder Sign up for Email Alert
National Security Telecommunications Advisory Committee (1 Document)	Docket Folder	NCS-2009-0005	Open Docket Folder Sign up for Email Alert
Notice of Meeting of the President's National Security Telecommunications Advisory Committee (NSTAC) (1 Document)	Docket Folder	NCS-2010-0001	Open Docket Folder Sign up for Email Alert
Recently Posted NSF Rules and Notices. (3 Documents)	Docket Folder	NSF_FRDOC_0001	Open Docket Folder Sign up for Email Alert
Recently Posted NTIA Rules and Notices. (5 Documents)	Docket Folder	NTIA_FRDOC_0001	Open Docket Folder Sign up for Email Alert
Recently Posted OPM Rules and Notices. (1 Document)	Docket Folder	OPM_FRDOC_0001	Open Docket Folder Sign up for Email Alert
Copyright Policy, Creativity, and Innovation in the Internet Economy (1 Document)	Docket Folder	PTO-C-2010-0041	Open Docket Folder Sign up for Email Alert
Agency Information Collection Activities; Proposals, Submissions, and Approvals (1 Document)	Docket Folder	TVA-2010-0009	Open Docket Folder Sign up for Email Alert
Agency Information Collection Activities; Proposals, Submissions, and Approvals (1 Document)	Docket Folder	TVA-2010-0013	Open Docket Folder Sign up for Email Alert
Agency Information Collection Activities; Proposals, Submissions, and Approvals (1 Document)	Docket Folder	TVA-2010-0015	Open Docket Folder Sign up for Email Alert
Recently Posted USDA Rules and Notices. (1 Document)	Docket Folder	USDA_FRDOC_0001	Open Docket Folder Sign up for Email Alert

Page 1 of 1 Displaying 1 - 29 of 29

Search Results

New Search Search Within Results Search Advanced Search

Too many results? Narrow them here:

Agency

Find Agency:

- DARS (2)
- DHS (5)
- DOE (2)
- DOS (2)

Document Type

- Public Submissions (76)
- Other (3)
- Supporting & Related Materials (14)
- Notices
- Rules
- Proposed Rules

Docket Type

- Rulemaking (6)
- Nonrulemaking (58)

Comment Period

- Open (1)
- Closed (72)

Comment Period

From: MM/DD/YY

To: MM/DD/YY

Posted Date

From: 01/01/10

To: 09/14/10

73 results for ""cyber security""

Records Per Page: 50

View By Relevance | View By Docket Folder

Title	Document Type	ID	Actions
Safeguarding Unclassified Information (2008-D028) (2 Documents)	Docket Folder	DARS-2010-0012	Open Docket Folder Sign up for Email Alert
Office of the Secretary; Published Privacy Impact Assessments on the Web (1 Document)	Docket Folder	DHS-2009-0029	Open Docket Folder Sign up for Email Alert
Notice of Public Meeting of the DHS Data Privacy and Integrity Advisory Committee (1 Document)	Docket Folder	DHS-2010-0009	Open Docket Folder Sign up for Email Alert
New Information Collection Request, Sector-Specific Agency Executive Management Office Meeting Registration (1 Document)	Docket Folder	DHS-2010-0019	Open Docket Folder Sign up for Email Alert
Agency Information Collection Activities: Submission for Review; Information Collection Request for the Department of Homeland Security (DHS) Science and Technology Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT) program - 60-day Notice (1 Document)	Docket Folder	DHS-2010-0043	Open Docket Folder Sign up for Email Alert
PREDICT (1 Document)	Docket Folder	DHS-2010-0073	Open Docket Folder Sign up for Email Alert
This docket contains Federal Register Notices from the DOE FDMS Sandbox. (1 Document)	Docket Folder	DOE-HQ-2009-0003	Open Docket Folder Sign up for Email Alert
Implementing the National Broadband Plan (1 Document)	Docket Folder	DOE-HQ-2010-0012	Open Docket Folder Sign up for Email Alert
Meeting of Advisory Committee on International Communications and Information Policy (1 Documcnt)	Docket Folder	DOS-2010-0002	Open Docket Folder Sign up for Email Alert
State-68, Office of the Coordinator for Reconstruction and Stabilization Records (1 Document)	Docket Folder	DOS-2010-0361	Open Docket Folder Sign up for Email Alert
Agency Information Collection Activity Seeking OMB Approval (1 Document)	Docket Folder	FAA-2010-0013	Open Docket Folder Sign up for Email Alert

Meetings; Sunshine Act (1 Document)	Docket Folder	FCC-2010-0109	Open Docket Folder Sign up for Email Alert
Cyber Security Certification Program (1 Document)	Docket Folder	FCC-2010-0138	Open Docket Folder Sign up for Email Alert
Framework for Broadband Internet Service (1 Document)	Docket Folder	FCC-2010-0184	Open Docket Folder Sign up for Email Alert
Notice of Federal Advisory Committee Meeting; National Advisory Council (1 Document)	Docket Folder	FEMA-2007-0008	Open Docket Folder Sign up for Email Alert
Commission Information Collection Activities (FERC-729); Comment Request; Submitted for OMB Review (1 Document)	Docket Folder	FERC-2010-0156	Open Docket Folder Sign up for Email Alert
Combined Notice of Filings (1 Document)	Docket Folder	FERC-2010-0598	Open Docket Folder Sign up for Email Alert
Power Reactor Security Requirements (1 Document)	Docket Folder	NRC-2008-0019	Open Docket Folder Sign up for Email Alert
Memorandum of Understanding Between the U.S. Nuclear Regulatory Commission and the North American Electric Reliability Corporation (1 Document)	Docket Folder	NRC-2010-0007	Open Docket Folder Sign up for Email Alert
Issuance and Availability of Final Regulatory Guide (1 Document)	Docket Folder	NRC-2010-0009	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0019	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0020	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0021	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0023	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0024	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0026	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0030	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact - Wolf Creek Nuclear Operating Corporation (1 Document)	Docket Folder	NRC-2010-0032	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0043	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0045	Open Docket Folder Sign up for Email Alert

Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0046	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0049	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0059	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0060	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (2 Documents)	Docket Folder	NRC-2010-0061	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0062	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0066	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0067	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0079	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0082	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0084	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0087	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0094	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0099	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0100	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0101	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0105	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0108	Open Docket Folder Sign up for Email Alert

Page 1 of 2 Displaying 1 - 50 of 73

Search Results

New Search Search Within Results

Search Advanced Search

Too many results? Narrow them here:

Agency

Find Agency:

- DARS (2)
- DHS (5)
- DOE (2)
- DOS (2)

Document Type

- Public Submissions (76)
- Other (3)
- Supporting & Related Materials (14)
- Notices
- Rules
- Proposed Rules

Docket Type

- Rulemaking (6)
- Nonrulemaking (58)

Comment Period

- Open (1)
- Closed (72)

Comment Period

From: MM/DD/YY

To: MM/DD/YY

Posted Date

From: 01/01/10

To: 09/14/10

73 results for ""cyber security""

Records Per Page: 50

View By Relevance | View By Docket Folder

Title	Document Type	ID	Actions
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0109	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0110	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0111	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0114	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0123	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0124	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0125	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0127	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0128	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0136	Open Docket Folder Sign up for Email Alert
Environmental Assessment and Finding of No Significant Impact (1 Document)	Docket Folder	NRC-2010-0137	Open Docket Folder Sign up for Email Alert
Proposed NUREG-0800, Standard Review Plan Section 13.6.6, Draft Revision 0 on Cyber Security Plan (1 Document)	Docket Folder	NRC-2010-0184	Open Docket Folder Sign up for Email Alert

Draft Regulatory Guide: Issuance, Availability (1 Document)	Docket Folder	NRC-2010-0216	Open Docket Folder Sign up for Email Alert
Applications and Amendments to Facility Operating Licenses Involving No Significant Hazards Considerations (1 Document)	Docket Folder	NRC-2010-0272	Open Docket Folder Sign up for Email Alert
Applications and Amendments to Facility Operating Licenses Involving Proposed No Significant Hazards Considerations (1 Document)	Docket Folder	NRC-2010-0279	Open Docket Folder Sign up for Email Alert
Recently Posted NTIA Rules and Notices. (2 Documents)	Docket Folder	NTIA_FRDOC_0001	Open Docket Folder Sign up for Email Alert
Work Reserved for Performance by Federal Government Employees (1 Document)	Docket Folder	OFPP-2010-0001	Open Docket Folder Sign up for Email Alert
Recently Posted OPM Rules and Notices. (2 Documents)	Docket Folder	OPM_FRDOC_0001	Open Docket Folder Sign up for Email Alert
Consumer Interface with the Smart Grid (1 Document)	Docket Folder	OSTP-2010-0003	Open Docket Folder Sign up for Email Alert
Consumer Interface with the Smart Grid (1 Document)	Docket Folder	OSTP-2010-0004	Open Docket Folder Sign up for Email Alert
Chemical (Drug and Alcohol) Testing (1 Document)	Docket Folder	USCG-2009-0973	Open Docket Folder Sign up for Email Alert

Page 2 of 2 Displaying 51 - 73 of 73