Before the
Department of Commerce

In the Matter of	)	
	)	
Cybersecurity, Innovation and the Internet Economy	)	**Docket No.: 100721305–0305–01**
	)	
	)	

COMMENTS OF
THE UNITED STATES TELECOM ASSOCIATION

USTelecom is pleased to provide these comments to the Department of Commerce (Department) in the above referenced proceeding, regarding the comprehensive review of the nexus between cybersecurity challenges in the commercial sector and innovation in the Internet economy.[1] The Internet in the United States is a tremendous success story. It has developed with speed and scope unparalleled by any prior network technology, and, with an estimated half trillion dollars in investment predominantly from the private sector,[2] has created jobs, spurred innovation, and revolutionized the way Americans learn, work, communicate, conduct commerce and increasingly engage with local, state, and federal government. USTelecom has previously commented in great detail on the economic impact of the broadband-fueled information and communications technologies (ICT) sector, and how it has become a major engine of economic

[1] Cybersecurity, Innovation and the Internet Economy, 74 Fed. Reg. 44,216, (July 28, 2010) (*Notice*).

[2] *See*, United States Department of Commerce, National Telecommunications and Information Administration (NTIA), Networked Nation: Broadband in America 2007 (January 2008), pp. 32-34. The NTIA data include payments for wireless spectrum licenses. Wireless, capital expenditures for 2000-2002 were derived by taking the difference of cumulative capital expenditures published by the Federal Communications Commission in its Tenth Annual Report and Analysis of Competitive Market Conditions with Respect to Commercial Mobile Services (FCC-05-173) (Released September 30, 2005), Table 1 at p. 80.

output and growth.[3] While the ICT sector represents only a portion of cybersecurity stakeholders, its impact on the nation's economy is significant.

Today's cyber environment is a highly complex ecosystem consisting of a global set of stakeholders engaged in an evolving system of multifaceted interactions. Telecommunications carriers play a central – but not exclusive – role in this diverse ecosystem, where the actions of a wide variety of independent entities can directly impact other stakeholders in the network. USTelecom believes that increased cybersecurity can best be achieved through greater coordination at the federal level of governmental cybersecurity efforts, availability of targeted incentives that enable greater cybersecurity investment, and increased public awareness on cybersecurity issues.

I. Greater Coordination of Federal Cybersecurity Efforts is Needed for all Federal Agency Stakeholders.

USTelecom has commented at length about the existing robust public-private mechanism that is addressing cyber incident management and coordination.[4] These joint efforts are designed to address both strategic and operational aspects of cybersecurity risk containment. Complementing these initiatives, as the Department considers the record in this proceeding, it

[3] *See e.g.*, Comments of USTelecom at the Federal Communications Commission (FCC), *Framework for Broadband Internet Service*, pp. 1 – 26, GN Docket No. 10-127 (submitted July 15, 2010). For example, the ICT sector contributed $902 billion in GDP in 2007 – making this sector among the top contributing sectors in the U.S. economy and the primary driver of real, inflation-adjusted growth. In 2008, U.S. firms invested $455 billion in ICT, representing 22% of total investment across the entire economy. Broadband providers alone invested over $64 billion in 2008 and, despite a relatively small decline due to macroeconomic pressures, broadband providers are projected to invest an average of approximately $60 billion per year for the next several years. *See*, Patrick S. Brogan, United States Telecom Association, New York Law School Media Law & Policy, Volume 18, Number II (Spring 2009) at pp. 163-165. *USTelecom FCC Comments*, p. 12.

[4] *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*).

should acknowledge the importance of the federal government to ensure greater coordination at the federal level of governmental cybersecurity efforts.

In particular, there is 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 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 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 certain proceedings that have in fact been initiated by federal agencies, thereby further confusing relevant stakeholders in these proceedings. For example, Regulations.gov does not list a recently initiated FCC proceeding regarding the "creation of a Cybersecurity Roadmap to identify vulnerabilities to communications networks or end-users and to develop countermeasures and solutions in preparation for, and response to, cyber threats and attacks in coordination with federal partners."[5]

This is not to say that these agencies should refrain from engaging in cybersecurity issues. Rather, there needs to be one central authority 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

[5] FCC Public Notice, *FCC Seeks Public Comment On National Broadband Plan Recommendation To Create A Cybersecurity Roadmap*, DA 10-1354 (released August 9, 2010).

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."[6]

II. Cybersecurity can be Enhanced with Targeted Incentives Throughout the Cyber Ecosystem.

A critical first step in effectively addressing cybersecurity issues is for stakeholders to acknowledge the diversity of the cyber-environment, which is characterized by a multiplicity in technologies and systems, an international reach, an extraordinarily dynamic information technology industry, and rapid evolution of cyber threats. Different segments of this ecosystem often have varying motivations and incentives with respect to cyberspace security.

Within the Internet ecosystem, private companies' business models are fully dependent on having secure, resilient and reliable services. Security flaws in these services result in private companies losing customers and business. As a result, businesses are taking substantial – and costly – measures to ensure they remain competitive and viable in today's marketplace. In the case of network providers, such guarantees in level of service are routinely embodied in service level agreements (SLAs) with their enterprise customers. SLAs are of fundamental importance in today's business environment, where an established level of service is formally defined, and network providers are under a contractual obligation to meet their commitments.

But through an effective positive incentives program, the federal government can help facilitate broader adoption of sound cybersecurity practices across *all* critical infrastructure and

[6] 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.

key resources (CIKR) sectors and within the federal government's own operations. The government should seek to encourage the broader adoption of cybersecurity practices that have already been demonstrated to be effective, while continuing to adapt existing best practices to keep pace with changing cybersecurity developments.

Given the diverse nature of the ICT sector, as well as the rapid pace with which cyber threats are evolving, any incentive program must avoid locking providers into non-flexible and prescriptive mandates. Instead, the government should encourage the use of best practices, which are developed using an ongoing, dynamic, and practical consensus process that moves at a more rapid pace that better corresponds with the dynamic nature of the cybersecurity environment. USTelecom has commented at length on the tremendous value and availability of best practices.[7]

There are a number of positive incentives the federal government could consider to foster increased cybersecurity. The Cross Sector Cyber Security Working Group[8] has identified several valuable incentives that the federal government could consider to enhance the nation's cybersecurity. For example, it proposes tax incentives to help improve cybersecurity, as well as direct funding and/or grants for cybersecurity research and development. It also recommends an evaluation of the existing cybersecurity landscape in order to identify areas where existing regulatory regimes could be

[7] *See e.g.*, *See e.g.*, Comments of USTelecom at the FCC, *Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload*, pp. 4 – 8, 15 – 16, PS Docket No. 10-92 (submitted June 25, 2010) (*USTelecom Network Survivability Comments*); *see also*, *USTelecom Cyber Certification Comments*, pp. 15 – 16.

[8] The Cross Sector Cyber Security Working Group (CSCSWG) was established by the Department of Homeland Security in the Spring of 2007 to address cross sector cyber risk and explore interdependencies. The working group serves as a forum to bring government and the private sector together to address common cyber security elements across the 17 critical infrastructure and key resource sectors. *See*, DHS News Release website, *Remarks of Cybersecurity and Communications Assistant Secretary Greg Garcia at the National Cyber Security Awareness Month Kick-Off Summit*, October 1, 2007 (available at: http://www.dhs.gov/xnews/releases/pr_1191270671928.shtm) (visited September 20, 2010).

streamlined to alleviate any duplication and ambiguities. Taken as a whole, such incentives could bridge the gap between what private sector business plans can support for cybersecurity investment and what might be needed to achieve additional cybersecurity enhancements desired by policymakers.

III. 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.[9] 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.[10]

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

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

---

[9] 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).

[10] *See* White House Report, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 29, 2009, p. 37 (identifying as a near term action plan the initiation of a national public awareness and education campaign to promote cybersecurity).

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."[11] 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.[12]

In the cybersecurity context, the federal government could focus on raising consumer and business awareness on issues relating to cybersecurity. Such outreach could emphasize 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.[13]

---

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

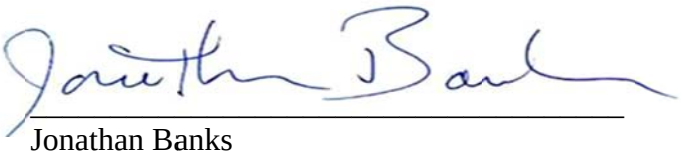
[12] Ad Council website (available at: http://www.adcouncil.org/default.aspx?id=68) (visited September 8, 2010).

[13] 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 September 20, 2010).

IV. Conclusion

USTelecom strongly supports ongoing efforts to secure the nation's critical communications from cybersecurity vulnerabilities. USTelecom believes that increased cybersecurity can best be achieved through greater coordination at the federal level of governmental cybersecurity efforts, availability of targeted incentives that enable greater cybersecurity investment, and increased public awareness on cybersecurity issues.

Respectfully submitted,
UNITED STATES TELECOM ASSOCIATION

By: 

Jonathan Banks
Robert Mayer
Kevin Rupy

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

September 20, 2010

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 Document)	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