—INFRASTRUCTURE and FEDERAL FACILITIES SECURITY—

AIRLINE SECURITY. U.S. Congress. Senate. Committee on Appropriations. Subcommittee on Transportation and Related Agencies; House. Committee on Appropriations. Subcommittee on Transportation and Related Agencies. 107th Congress, 1st Session, 20 September 2001. Washington, DC: U.S. Government Printing Office, 2002. 77p. [Joint Hearing].

SuDoc# Y 4. AP 6/2: S.HRG.107-480

> This special joint hearing of both the House and Senate Appropriations Subcommittees on Transportation and Related Agencies, held just nine days following the terrorist attacks on New York and Washington, examines the safety of the nation's airways, and potential measures, such as strengthened cockpit doors to enhance its safety.

Online

http://purl.access.gpo.gov/GPO/LPS20340

http://purl.access.gpo.gov/GPO/LPS20341 (PDF)

AIRPORT BAGGAGE SCREENING: MEETING GOALS AND ENSURING SAFETY—ARE WE ON TARGET? U.S. Congress. House. Committee on Government Reform. 107th Congress, 2nd Session, 7 August 2002. Washington, DC: U.S. Government Printing Office, 2002. 74p. [Hearing].

SuDoc# Y 4. G 74/7: AI 7/30

> "This hearing is being held to address the looming deadline that we have before us for screening checked baggage. Before September 11th, we did not have a system for screening checked baggage for bombs. We had a vulnerability that we were not addressing … Last fall, we passed the Aviation and Transportation Security Act. It set a deadline of December 31st this year to have explosive detecting machines up and running at every airport."

Online

http://purl.access.gpo.gov/GPO/LPS26051 (PDF)

AIRPORT PASSENGER SCREENING: PRELIMINARY OBSERVATIONS ON PROGRESS MADE AND CHALLENGES REMAINING. U.S. General Accounting Office. September 2003. Washington, DC: U.S. General Accounting Office, 2003. 24p. [Report].

SuDoc# GA 1.13: GAO-03-1173

> "…GAO is conducting an ongoing evaluation of TSA's [Transportation Security Administration] efforts to (1) ensure that passenger screeners are effectively trained and supervised, (2) measure screener performance in detecting threat objects, and (3) implement and evaluate the contract screening pilot program."

Online

http://www.gao.gov/cgi-bin/getrpt?GAO-03-1173 (PDF)

AIRPORT SECURITY (ORLANDO, FLORIDA). U.S. Congress. House. Committee on Transportation and Infrastructure. Subcommittee on Aviation. 107th Congress, 2nd Session, 17 September 2002. Washington, DC: U.S. Government Printing Office, 2002. 127p. [Hearing].

SuDoc# Y 4. T 68/2: 107-96

> "Unfortunately, some of the critical elements of developing a seamless transportation security system have not been coming together as smoothly as we would like. Today's hearing will focus on some of the problems that we have experienced in our initial attempts to develop a new passenger screening force…"

ARMING FLIGHT CREWS AGAINST TERRORIST ACTS. U.S. Congress. House. Committee on Transportation and Infrastructure. Subcommittee on Aviation. 107th Congress, 2nd Session, 2 May 2002. Washington, DC: U.S. Government Printing Office, 2002. 138p. [Hearing].

SuDoc# Y 4. T 68/2: 107-80

> "The question here is the last line of defense, and that's the pilot in the cockpit. Why should a pilot be denied the ability to use all reasonable force and methods for self-defense? We not only owe this to the pilot, but we owe this to our crew and the passengers. The pilot should at least have a fighting chance. If any of the pilots on September 11th had had this right and were armed, that day, in fact, would have been quite different … for those who are squeamish or concerned about a small caliber highly regulated weapon being fired at 30,000 feet, they should realize, again, that our last option today is an F-16 firing an air-to-air missile to bring down a hijacked passenger aircraft."

AVIATION SECURITY. U.S. Congress. House. Committee on Public Works and Transportation. Subcommittee on Aviation. 101st Congress, 1st Session, 21 March 1989. Washington, DC: U.S. Government Printing Office, 1989. 419p. [Hearing].

SuDoc# Y 4. P 96/11: 101-14

> "To improve aviation security by requiring the installation and use of certain explosive detection equipment at certain airports located outside the United States and by providing assistance for the acquisition of such equipment…"

AVIATION SECURITY. U.S. Congress. House. Committee on Transportation and Infrastructure. Subcommittee on Aviation. 107th Congress, 2nd Session, 23 July 2002. Washington, DC: U.S. Government Printing Office, 2002. 145p. [Hearing].

SuDoc# Y 4. T 68/2: 107-91

> "While the Administrator of the Transportation Security Administration will change, we must realistically reassess both the effectiveness, the cost, and the factual ability to meet arbitrary future deadlines we have imposed … the Transportation Security Administration has been consumed with constructing an army of more than 30,000 Federal workers, and those are just screening workers. And right now if we look at it, we have only three airports that are totally federalized and some 2,475 persons hired."

AVIATION SECURITY AND ANTI-TERRORISM EFFORTS. U.S. Congress. House. Committee on Transportation and Infrastructure. Subcommittee on Aviation. 104th Congress, 2nd Session, 11 September 1996. Washington, DC: U.S. Government Printing Office, 1997. 205p. [Hearing].

SuDoc# Y 4. T 68/2: 104-65

> "…there has been great concern regarding an increasing threat of terrorism, as well as the state of aviation security here in the United States. Although security measures have been successful against the major historical priority of deterring aircraft hijacking, the emergence of the threat of sophisticated domestic and international terrorism now requires a review of our core security activities."

AVIATION SECURITY AND THE FUTURE OF THE AVIATION INDUSTRY. U.S. Congress. House. Committee on Transportation and Infrastructure. Subcommittee on Aviation. 107th Congress, 1st Session, 21 & 25 September 2001. Washington, DC: U.S. Government Printing Office, 2001. 681p. [Hearing].

SuDoc# Y 4. T 68/2: 107-47

> "…the horrific tragedy on September 11 demonstrated several failures. First, our Federal intelligence system failed. Clearly we need to have better ability to penetrate terrorist organizations, and keep terrorists out of our country and certainly out of our airports and off of our airplanes. Next, somehow our Federal visa and immigration systems also failed dramatically."

AVIATION SECURITY (FOCUSING ON TRAINING AND RETENTION OF SCREENERS). U.S. Congress. House. Committee on Transportation and Infrastructure. Subcommittee on Aviation. 106th Congress, 2nd Session, 16 March 2000. Washington, DC: U.S. Government Printing Office, 2000. 144p. [Hearing].

SuDoc# Y 4. T 68/2: 106-77

> "The public does have a right to be concerned, because inadequate training and low morale among screeners threaten safety and security in the skies, and the men and women who stand at security check points are forced to work long, constant hours at minimum wage."

AVIATION SECURITY: PROGRESS SINCE SEPTEMBER 11, 2001, AND THE CHALLENGES AHEAD: STATEMENT OF GERALD L. DILLINGHAM, DIRECTOR, CIVIL AVIATION ISSUES. U.S. General Accounting Office. 9 September 2003. Washington, DC: U.S. General Accounting Office, 2003. [Testimony].

SuDoc# GA 1.5/2: GAO-03-1150 T

> "Since September 11, 2001, TSA has made considerable progress in meeting congressional mandates designed to increase aviation security. By the end of 2002, the agency had hired and deployed about 65,000 passenger and baggage screeners, federal air marshals, and others, and it was using explosives detection equipment to screen about 90 percent of all checked baggage. TSA is also initiating or developing efforts that focus on the use of technology and information to advance security. One effort under development, the next-generation Computer-Assisted Passenger Prescreening System (CAPPS II), would use national security and commercial databases to identify passengers who could pose risks for additional screening. Concerns about privacy rights will need to be addressed as this system moves toward implementation."

Online

http://www.gao.gov/cgi-bin/getrpt?GAO-03-1150T (PDF)

http://www.gao.gov/new.items/d031150t.pdf (PDF)

AVIATION SECURITY: TECHNOLOGY'S ROLE IN ADDRESSING VULNERABILITIES: STATEMENT OF KEITH O. FULTZ, ASSISTANT COMPTROLLER GENERAL, RESOURCES, COMMUNITY, AND ECONOMIC DEVELOPMENT DIVISION. U.S. General Accounting Office. 19 September 1996. Washington, DC: U.S. General Accounting Office, 1996. 13p. [Testimony].

SuDoc# GA 1.5/2: T-RCED/NSIAD-96-262

> "If further incidents occur, pubic fear and anxiety will escalate, and the economic well-being of the aviation industry will suffer because of reductions in travel and shipment of goods. Given the persistence of long-standing vulnerabilities and the increased threat to civil aviation, we believe that corrective actions need to be undertaken immediately. These actions need a unified effort from the highest levels of the government to address this national issue."

Online

http://purl.access.gpo.gov/GPO/LPS15016 (PDF)

AVIATION SECURITY: URGENT ISSUES NEED TO BE ADDRESSED: STATEMENT OF KEITH O. FULTZ, ASSISTANT COMPTROLLER GENERAL, RESOURCES, COMMUNITY, AND ECONOMIC DEVELOPMENT DIVISION. U.S. General Accounting Office. 11 September 1996. Washington, DC: U.S. General Accounting Office, 1996. 14p. [Testimony].

SuDoc# GA 1.5/2: T-RCED/NSIAD-96-251

> "Terrorists' activities are continually evolving and present unique challenges to FAA and law enforcement agencies. We reported in March 1996 that the bombing of Philippine Airlines flight 434 in December 1994 illustrated the potential extent of terrorists' motivation and capabilities as well as the attractiveness of aviation as a target for terrorists. According to information that was accidentally uncovered in January 1995, this bombing was a rehearsal for multiple attacks on specific U.S. flights in Asia."

Online

http://purl.access.gpo.gov/GPO/LPS15018 (PDF)

CARGO CONTAINERS: THE NEXT TERRORIST TARGET? U.S. Congress. Senate. Committee on Governmental Affairs. 108th Congress, 1st Session, 20 March 2003. Washington, DC: U.S. Government Printing Office, 2003. 106p. [Hearing].

SuDoc# Y 4. G 74/9: S.HRG. 108-55

> "There are more than 12 million cargo containers in the worldwide inventory. These containers move back and forth among major seaports more than 200 million times a year. Every day, more than 21,000 containers arrive at American seaports from foreign countries filled with consumer goods … in fact, about 90 percent of U.S.-bound cargo moves by container. We must ensure that these containers carry nothing more dangerous than sneakers or sporting goods, not 'dirty bombs' or even Al Qaeda terrorists."

Online

http://purl.access.gpo.gov/GPO/LPS34709 (PDF)

CHECKED BAGGAGE SCREENING SYSTEMS—PLANNING FOR THE DECEMBER 31, 2002 DEADLINE. U.S. Congress. House. Committee on Transportation and Infrastructure. Subcommittee on Aviation. 107th Congress, 1st Session, 7 December 2001. Washington, DC: U.S. Government Printing Office, 2002. 110p. [Hearing].

SuDoc# Y 4. T 68/2: 107-58

> "To meet the December 31, 2002, deadline, some experts have estimated that it may require more than 2,000 machines at a cost which could exceed some $5 billion … There will be substantial costs, additional costs to man this equipment. There is no

doubt that meeting the deadline for deployment will indeed be a difficult task. Few agencies have ever been directed to undertake such a formidable assignment."

COMBATING TERRORISM: ACTIONS NEEDED TO IMPROVE FORCE PROTECTION FOR DOD DEPLOYMENTS THROUGH DOMESTIC SEAPORTS. U.S. General Accounting Office. October 2002. Washington, DC: U.S. General Accounting Office, 2002. 35p. [Report].

SuDoc# GA 1.13: GAO-03-15

> "The security environment at strategic seaports remains uncertain because comprehensive assessments of threats, vulnerabilities, and critical port infrastructure and functions have not been completed, and no effective mechanism exists to coordinate and disseminate threat information at the seaports. These conditions compound the already difficult task of protecting deploying forces and increase the risk that threats—both traditional and nontraditional ones— may not be recognized or that threat information may not be communicated in a timely manner to all relevant organizations."

Online

http://www.gao.gov/cgi-bin/getrpt?GAO-03-15 (PDF)

http://www.gao.gov/new.items/d0315.pdf (PDF)

COMPUTER SECURITY: ARE WE PREPARED FOR CYBERWAR? U.S. Congress. House. Committee on Government Reform. Subcommittee on Government Management, Information, and Technology. 106th Congress, 2nd Session, 9 March 2000. Washington, DC: U.S. Government Printing Office, 2000. 201p. [Hearing].

SuDoc# Y 4. G 74/7: SE 2/16

> "The dimension and scope of … cyber attacks … What efforts are being undertaken toward solving the problem … What the Federal Government is doing to address this problem."

Online

http://purl.access.gpo.gov/GPO/LPS8942

http://purl.access.gpo.gov/GPO/LPS8943 (PDF)

COMPUTER SECURITY IN THE FEDERAL GOVERNMENT: HOW DO THE AGENCIES RATE? U.S. Congress. House. Committee on Government Reform. Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. 107th Congress, 2nd Session, 19 November 2003. Washington, DC: U.S. Government Printing Office, 2003. 116p. [Hearing].

SuDoc# Y 4. G 74/7: C 73/40/2002

> "Last year the number of cyber attacks rose 71 percent above the previous year. In addition, they are more complex, affecting government and nongovernment computers alike. Earlier this year, a British computer administrator penetrated 100 U.S. military computers, shutting down networks and corrupting data at the National Aeronautics and Space Administration and at the Pentagon. Equally disturbing, the hacker successfully attacked these sensitive systems by using software that was readily available on the Internet. Threats such as this demand that the Federal Government move quickly to protect its critical computer systems."

Online

http://purl.access.gpo.gov/GPO/LPS39261 (PDF)

COMPUTER SECURITY IN THE FEDERAL GOVERNMENT: HOW DO THE AGENCIES RATE? U.S. Congress. House. Committee on Government Reform. Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. 107th Congress, 1st Session, 9 November 2001. Washington, DC: U.S. Government Printing Office, 2002. 70p. [Hearing].

SuDoc# Y 4. G 74/7: C 73/40

> "Federal agencies rely on computer systems to support critical operations that are essential to the health and well-being of millions of Americans. National defense, emergency services, tax collection, and benefit payments all rely on automated systems and electronically stored information. Without proper protection, the vast amount of sensitive information stored on executive branch computers could be compromised and the systems themselves subject to malicious attack."

Online

http://purl.access.gpo.gov/GPO/LPS24854 (PDF)

CONTAINER SECURITY: EXPANSION OF KEY CUSTOMS PROGRAMS WILL REQUIRE GREATER ATTENTION TO CRITICAL SUCCESS FACTORS. U.S. General Accounting Office. July 2003. Washington, DC: U.S. General Accounting Office, 2003. 56p. [Report].

SuDoc# GA 1.13: GAO-03-770

> "Since September 11, 2001, concern has increased that terrorists could smuggle weapons of mass destruction in the 7 million ocean containers that arrive annually at U.S. seaports. In response to this concern, the U.S. Customs Service (Customs) implemented the Container Security Initiative (CSI) to screen for high-risk containers at overseas ports and Customs-Trade Partnership Against Terrorism (C-TPAT) to improve global supply chain security in the private sector. GAO (1) describes the purpose and elements of these new programs, (2) examines Customs' implementation of CSI and C-TPAT during the first year, and (3) assesses the extent to which Customs has focused on factors critical to the programs' long-term success and accountability."

Online

http://purl.access.gpo.gov/GPO/LPS37731 (PDF)

http://www.gao.gov/cgi-bin/getrpt?GAO-03-770 (PDF)

http://www.gao.gov/new.items/d03770.pdf (PDF)

COUNTERTERRORISM AND INFRASTRUCTURE PROTECTION. U.S. Congress. Senate. Committee on Appropriations. Subcommittee on Commerce, Justice, State, the Judiciary, and Related Agencies. 106th Congress, 2nd Session, 1999. Washington, DC: U.S. Government Printing Office, 1999. 79p. [Special Hearing].

SuDoc# Y 4. AP 6/2: S.HRG.106-145

> Agency cooperation and preparedness, infrastructure protection against terrorism, terrorism budget strategy, partnership between the Federal Government and local law enforcement, threat of cyber attack, preventing and responding to terrorism, embassy security, clarification of authority to activate the National Guard, Top Off Exercise, Y2K impact, preparations for possible Y2K terrorist activities.

CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES. Office of the President (William J. Clinton). October 1997. Washington, DC: President's Commission on Critical Infrastructure Protection, 1997. 174p. [Report].

SuDoc# PR 42.8: IN 3/C 86

> "Physical vulnerabilities to man-made threats, such as arson and bombs, are likewise not new. But physical vulnerabilities take on added significance as new capabilities to exploit them emerge, including chemical, biological, and even nuclear weapons. As weapons of mass destruction proliferate, the likelihood of their use by terrorists increases. Terrorist attacks have typically been against single targets—individuals, buildings, or institutions. Today, more sophisticated physical attacks may also exploit the emerging vulnerabilities associated with the complexity and interconnectedness of our infrastructures."

Online

http://purl.access.gpo.gov/GPO/LPS15260 (PDF)

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION: THE THREAT IS REAL. U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Technology, Terrorism, and Government Information. 106th Congress, 1st Session, 6 October 1999. Washington, DC: U.S. Government Printing Office, 2001. 59p. [Hearing].

SuDoc# Y 4. J 89/2: S.HRG.106-858

> "Because of the interrelated nature of our critical infrastructure systems, today's terrorist has the potential to do with a keyboard what in the last world war might have taken a squadron of bombers to accomplish. At stake are not only the information systems upon which we rely, but the electric power grid, the public switch communications network, the air traffic control system, the banking system, rail transport, oil and gas distribution networks, and a host of other networks on which our national security and our way of life today depend."

Online

http://purl.access.gpo.gov/GPO/LPS10299

http://purl.access.gpo.gov/GPO/LPS10300 (PDF)

CRITICAL INFRASTRUCTURE: CONTROL SYSTEMS AND THE TERRORIST THREAT. Library of Congress. Dana A. Shea. 21 February 2003. Washington, DC: Congressional Research Service, Library of Congress, 2003. 14p. [Online Report].

SuDoc# LC 14.19/3: RL31534

> "The federal government has issued a warning regarding an increase in terrorist interest in the cyber-security of industrial control systems, citing both interest by international terrorist organizations in critical infrastructure and increases in cyber-attack on critical infrastructure computer systems. The potential consequences of a successful cyber-attack on critical infrastructure industrial control systems could be high, ranging from a temporary loss of service to catastrophic infrastructure failure affecting multiple states for an extended duration."

Online

http://www.fas.org/irp/crs/RL31534.pdf (PDF)

CRITICAL INFRASTRUCTURE INFORMATION DISCLOSURE AND HOMELAND SECURITY. Library of Congress. John D. Moteff and Gina Marie Stevens. 29 January 2003. Washington, DC: Congressional Research Service, Library of Congress, 2003. 19p. [Online Report].

SuDoc# LC 14.19/3: RL31547

> "One of the findings of the President's Commission on Critical Infrastructure Protection, established by President Clinton in 1996, was the need for the federal government and owners and operators of the nation's critical infrastructures to share information on vulnerabilities and threats. However, the Commission noted that owners and operators are reluctant to share confidential business information, and the government is reluctant to share information that might compromise intelligence sources or investigations."

Online

http://www.fas.org/sgp/crs/RL31547.pdf (PDF)

CRITICAL INFRASTRUCTURE PROTECTION: CHALLENGES FOR SELECTED AGENCIES AND INDUSTRY SECTORS. U.S. General Accounting Office. February 2003. Washington, DC: U.S. General Accounting Office, 2003. 71p. [Report].

SuDoc# GA 1.13: GAO-03-233

> "Federal efforts to protect our nation's critical public and private infrastructures have had mixed progress. GAO examined four specific agencies—the Departments of Health and Human Services (HHS), Energy, and Commerce, and the Environmental Protection Agency (EPA)—and found that the agencies have made progress in implementing several PDD 63 requirements…However, none of the agencies has fully implemented all requirements, including the fundamental processes of identifying agency assets that are critical to the nation and determining their dependencies on other public and private assets, as well as assessing these assets' vulnerabilities. In addition, though most agencies have tentatively identified their critical assets, these efforts could take years to complete given the current pace and estimated time and resource needs."

Online

http://purl.access.gpo.gov/GPO/LPS43947 (PDF)

CRITICAL INFRASTRUCTURE PROTECTION: EFFORTS OF THE FINANCIAL SERVICES SECTOR TO ADDRESS CYBER THREATS. U.S. General Accounting Office. January 2003. Washington, DC: U.S. Government Printing Office, 2003. 58p. [Report].

SuDoc# GA 1.13: GAO-03-173

> "GAO was asked to review (1) the general nature of the cyber threats faced by the financial services industry; (2) steps the financial services industry has taken to share information on and to address threats, vulnerabilities, and incidents; (3) the relationship between government and private sector efforts to protect the financial services industry's critical infrastructures; and (4) actions financial regulators have taken to address these cyber threats."

Online

http://purl.access.gpo.gov/GPO/LPS30025 (PDF)

CRITICAL INFRASTRUCTURE PROTECTION: FEDERAL EFFORTS REQUIRE A MORE COORDINATED AND COMPREHENSIVE APPROACH FOR PROTECTING INFORMATION SYSTEMS. U.S. General Accounting Office. July 2002. Washington, DC: U.S. General Accounting Office, 2002. 77p. [Report].

SuDoc# GA 1.13: GAO-02-474

> "At the federal level, cyber CIP activities are a component, perhaps the most critical, of a federal department or agency's overall information security program. Since September 1996, we have reported that poor information security is a widespread federal government problem with potentially devastating consequences … federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations."

Online

http://purl.access.gpo.gov/GPO/LPS34689 (PDF)

http://www.gao.gov/new.items/d02474.pdf (PDF)

CRITICAL INFRASTRUCTURE PROTECTION: TOWARD A NEW POLICY DIRECTIVE. U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Technology, Terrorism, and Government Information. 105th Congress, 2nd Session, 17 March; 10 June 1998. Washington, DC: U.S. Government Printing Office, 1998. 163p. [Hearing].

SuDoc# Y 4. J 89/2: S.HRG.105-763

> "As we will hear today, in the midst of tensions with Iraq, the United States experienced the most serious and aggressive set of intrusions ever detected into sensitive defense information systems. According to intelligence reports, foreign nations as well as terrorist groups are stepping up efforts to acquire offensive information warfare tools and techniques, and we still have no national strategy or policy to protect ourselves."

CRITICAL INFRASTRUCTURE PROTECTION: WHO'S IN CHARGE? U.S. Congress. Senate. Committee on Governmental Affairs. 107th Congress, 1st Session, 4 October 2001. Washington, DC: U.S. Government Printing Office, 2002. 105p. [Hearing].

SuDocs# Y 4. G 74/9: S.HRG.107-258

> "The terrorist attacks provide evidence that physical assaults can cause severe disruptions in the service and delivery of goods and products, triggering ripple effects throughout the Nation's economy, and more importantly damaging the faith of the people in the viability of the day-to-day functioning of the country."

Online

http://purl.access.gpo.gov/GPO/LPS22196

http://purl.access.gpo.gov/GPO/LPS22197 (PDF)

CRITICAL INFRASTRUCTURES: BACKGROUND, POLICY, AND IMPLEMENTATION. Library of Congress. John D. Moteff. 10 February 2003. Washington, DC: Congressional Research Service, Library of Congress, 2003. 32p. [Online Report].

SuDoc# LC 14.19/3: RL30153

> "Prior to September 11, critical infrastructure protection was synonymous with cyber security to many people. Consequently, this report discusses cyber related activities and issues. However, the terrorist attacks of September 11, and the subsequent anthrax attacks, demonstrate the need to reexamine physical protections and to integrate this into an overall critical infrastructure policy."

Online

http://www.fas.org/irp/crs/RL30153.pdf (PDF)

CRITICAL INFRASTRUCTURES: WHAT MAKES AN INFRASTRUCTURE CRITICAL? Library of Congress. John Moteff, Claudia Copeland and John Fischer. 29 January 2003. Washington, DC: Congressional Research Service, Library of Congress, 2002. 20p. [Online Report].

SuDoc# LC 14.19/3: RL31556

> "Executive Order 13010, signed by President Clinton on July 15, 1996, which established the President's Commission on Critical Infrastructure Protection, alluded to what makes an infrastructure critical: 'Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.' According to this Executive Order (EO) these infrastructures included: telecommunication systems; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; emergency services (including medical, police, fire, and rescue); and, continuity of government."

Online

http://www.fas.org/irp/crs/RL31556.pdf (PDF)

CYBER ATTACK: IMPROVING PREVENTION AND PROSECUTION. U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Technology, Terrorism, and Government Information. 106th Congress, 2nd Session, 21 April 2000. Washington, DC: U.S. Government Printing Office, 2001. 112p. [Hearing].

SuDoc# Y 4. J 89/2: S.HRG.106-838

> "Catching and punishing those who commit cyber crimes is essential for deterring future attacks. When a cyber attack occurs, it is not initially apparent whether the perpetrator is a mischievous teenager, a professional hacker, a terrorist group, or even a hostile nation. Law enforcement must be equipped with the resources and

> authorities necessary to swiftly trace a cyber attack back to its source and appropriately prosecute criminals."

<u>Online</u>

http://purl.access.gpo.gov/GPO/LPS10465

http://purl.access.gpo.gov/GPO/LPS10466 (PDF)

CYBER ATTACK: IS THE GOVERNMENT SAFE? U.S. Congress. Senate. Committee on Governmental Affairs. 106th Congress, 2nd Session, 2 March 2000. Washington, DC: U.S. Government Printing Office, 2000. 121p. [Hearing].

SuDoc# Y 4. G 74/9: S.HRG.106-486

> "Today, the Committee on Governmental Affairs is holding a hearing on the ability of the Federal Government to protect against and respond to potential cyber attacks … Numerous Governmental Affairs Committee hearings and General Accounting Office reports uncovered and identified systemic failures of government information systems, which highlighted our Nation's vulnerability to computer attacks from international and domestic terrorists, to crime rings, to everyday hackers."

<u>Online</u>

http://purl.access.gpo.gov/GPO/LPS5260

http://purl.access.gpo.gov/GPO/LPS5261 (PDF)

CYBER ATTACK: IS THE NATION AT RISK? U.S. Congress. Senate. Committee on Governmental Affairs. 105th Congress, 2nd Session, 24 June 1998. Washington, DC: U.S. Government Printing Office, 1998. 35p. [Hearing].

SuDoc# Y 4. G 74/9: S.HRG.105-614

> "Established terrorist groups are likely to view attacks against information systems as a means of striking at government, commercial, and industrial targets with little risk of being caught. Global proliferation of computer technology and the open availability of computer tools that can be used to attack other computers make it possible for terrorist groups to develop this capability without great difficulty."

CYBER ATTACKS: REMOVING ROADBLOCKS TO INVESTIGATION AND INFORMATION SHARING. U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Technology, Terrorism, and Government Information. 106th Congress, 2nd Session, 28 March 2000. Washington, DC: U.S. Government Printing Office, 2001. 82p. [Hearing].

SuDoc# Y 4. J 89/2: S.HRG.106-839

> "…overall protection from attack necessitates that information about cyber vulnerabilities, threats and attacks be communicated among companies and with government agencies. Cooperation among competitors, while adhering to underlying antitrust laws, is necessary to create information sharing and analysis centers in each portion of the private sector."

Online

http://purl.access.gpo.gov/GPO/LPS10391

http://purl.access.gpo.gov/GPO/LPS10392 (PDF)

CYBER ATTACKS: THE NATIONAL PROTECTION PLAN AND ITS PRIVACY IMPLICATIONS. U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Technology, Terrorism, and Government Information. 106th Congress, 2nd Session, 1 February 2000. Washington, DC: U.S. Government Printing Office, 2001. 79p. [Hearing].

SuDoc# Y 4. J 89/2: S.HRG.106-889

> "The reality is that doing nothing to enhance our cyber security, in fact, erodes the privacy and civil liberties of Americans by making public information accessible to any hacker with a computer and a modem … The National Plan's implementation must consider the reasonable privacy issues that must be discussed and appropriately balance them with security interests."

Online

http://purl.access.gpo.gov/GPO/LPS10960

http://purl.access.gpo.gov/GPO/LPS10961 (PDF)

CYBER SECURITY—HOW CAN WE PROTECT AMERICAN COMPUTER NETWORKS FROM ATTACK? U.S. Congress. House. Committee on Science. 107th Congress, 1st Session, 10 October 2001. Washington, DC: U.S. Government Printing Office, 2002. 79p. [Hearing].

SuDoc# Y 4. SCI 2: 107-41

> "…to examine the vulnerability of our Nation's computer infrastructure as well as research-related challenges and opportunities facing the Nation's computer networks. Testifying before the Committee will be witnesses representing industry, academic, government and non-profit organizations. Witnesses will comment on gaps in research and education in the computer security field. Since most of the information infrastructure in the United States is owned and controlled by the private sector, witnesses will also comment on ways to encourage collaborative approaches to shoring up our ability to predict, prevent, and mitigate attacks."

Online

http://purl.access.gpo.gov/GPO/LPS30707

CYBER SECURITY: PRIVATE-SECTOR EFFORTS ADDRESSING CYBER THREATS. U.S. Congress. House. Committee on Energy and Commerce. Subcommittee on Commerce, Trade, and Consumer Protection. 107th Congress, 1st Session, 15 November 2001. Washington, DC: U.S. Government Printing Office, 2002. 65p. [Hearing].

SuDoc# Y 4. C 73/8: 107-74

> "Since September 11, we have learned that terrorists do have the wherewithal to undertake the unexpected. Terrorists and their recruits also have grown up in the digital age and thus, most probably, possess the technical skills to undertake concerted and effective cyber attacks. And as the real and virtual worlds have become more closely intertwined, cyber terrorism can potentially engender greater pain and tragedy, and thus become more attractive to unscrupulous terrorists."

Online

http://purl.access.gpo.gov/GPO/LPS18117

http://purl.access.gpo.gov/GPO/LPS18118 (PDF)

CYBER SECURITY RESEARCH AND DEVELOPMENT. U.S. Congress. House. Committee on Science. 108th Congress, 1st Session, 14 May 2003. Washington, DC: U.S. Government Printing Office, 2003. 112p. [Hearing].

SuDoc# Y 4. SCI 2: 108-17

> "The hearing will address the following overarching questions: 1. What is the current status of federally-supported cyber security research and development programs in the United States? What level and types of effort are needed to meet existing and emerging cyber terrorism threats? 2. How are cyber security research and development activities coordinated among federal agencies? How are gaps in the research portfolio identified and filled? How will the new Department of Homeland Security affect the coordination process? How will it change the overall portfolio of programs? 3. What efforts are being made to develop a strong cyber security workforce and to establish and expand university educational and research programs related to cyber security? 4. How do the federal agencies work with industry on cyber security research and development efforts?"

Online

http://purl.access.gpo.gov/GPO/LPS40610

CYBER TERRORISM—A VIEW FROM THE GILMORE COMMISSION. U.S. Congress. House. Committee on Science. 107th Congress, 1st Session, 17 October 2001. Washington, DC: U.S. Government Printing Office, 2002. 81p. [Hearing].

SuDoc# Y 4. SCI 2: 107-40

> "Testifying before the committee will be The Honorable James S. Gilmore, III, Governor of the Commonwealth of Virginia and Chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. Governor Gilmore will assess the threats to our Nation's information infrastructure, describe the level of preparedness to address these threats, and describe steps that need to be taken to ensure that Federal, state, and local governments are prepared to respond."

CYBERTERRORISM: IS THE NATION'S CRITICAL INFRASTRUCTURE ADEQUATELY PROTECTED? U.S. Congress. House. Committee on Government Reform. Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. 107th Congress, 2nd Session, 24 July 2002. Washington, DC: U.S. Government Printing Office, 2003. 193p. [Hearing].

SuDoc# Y 4. G 74/7: C 99/2

> "In 1998, a 12-year-old boy successfully hacked into computer systems that controlled the Roosevelt Dam in Arizona. He could have opened the dam's floodgates and dumped nearly 500 billion gallons of water on the Arizona cities of Mesa and Tempe … in April 2000, an Australian hacker used his laptop computer and commercially available radio transmitter to gain control of a local sewage treatment facility. He intentionally released raw sewage into nearby parks and rivers on 46 occasions before he was caught. It is clear from these and other reports that the Nation's water, power, financial markets, and telecommunications systems could be similarly attacked."

Online

http://purl.access.gpo.gov/GPO/LPS34622 (PDF)

DEFENDING AMERICA'S CYBERSPACE: NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION. Office of the President (William J. Clinton). Washington, DC: The White House; U.S. Government Printing Office, 2000. 159p. [Report].

SuDoc# PR 42.8: IN 3/C 99

> "We know that the threat is real. Where once our opponents relied exclusively on bombs and bullets, hostile powers and terrorists can now turn a laptop computer into a potent weapon capable of doing enormous damage. If we are to continue to enjoy the benefits of the Information Age, preserve our security, and safeguard our economic well-being, we must protect our critical computer-controlled systems from attack."

Online

http://purl.access.gpo.gov/GPO/LPS5097 (PDF)

DEFENDING AMERICA'S CYBERSPACE: NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION (EXECUTIVE SUMMARY). Office of the President (William J. Clinton). Washington, DC: The White House; U.S. Government Printing Office, 2000. 32p. [Report Summary].

SuDoc# PR 42.8: IN 3/C 99/EXEC.SUM.

> "The National Plan for Information Systems Protection is the first major element of a more comprehensive effort. The Plan for cyber defense will evolve and be updated as we deepen our knowledge of our vulnerabilities and the emerging threats. It presents a comprehensive vision creating the necessary safeguards to protect the critical sectors of our economy, national security, public health, and safety."

Online

http://purl.access.gpo.gov/GPO/LPS5098 (PDF)

DEFENDING AMERICA'S TRANSPORTATION INFRASTRUCTURE. U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Crime and Drugs. 107th Congress, 1st Session, 16 October 2001. Washington, DC: U.S. Government Printing Office, 2002. 31p. [Hearing].

SuDoc# Y 4. J 89/2: S.HRG.107-612

> "These hearings will focus on the extent to which security vulnerabilities exist in non-aviation transportation. That is because today we need to anticipate the threat that may come not just in the belly of a plane, but in the hold of a ship or in the dark of a tunnel or the span of a bridge … Our modes of surface and sub-surface transportation may not be keeping up with the security advances that we are seeing in the air. For example, it has recently been reported that 98 percent of all cargo containers enter U.S. ports without any inspection."

Online

http://purl.access.gpo.gov/GPO/LPS22237

http://purl.access.gpo.gov/GPO/LPS22238 (PDF)

ELECTRICITY INFRASTRUCTURE. U.S. Congress. Senate. Committee on Energy and Natural Resources. 107th Congress, 2nd Session, 24 July 2002. Washington, DC: U.S. Government Printing Office, 2002. 63p. [Hearing].

SuDoc# Y 4. EN 2: S.HRG.107-783

> "Another critical aspect of our electricity infrastructure, especially in light of recent world events, is its ability to avoid disruption by physical or cyber threats. NERC, as the Information Sharing and Analysis Center (ISAC) for the electricity sector, works with federal, state, provincial and local organizations, and its Regions to monitor the activities under way to protect the physical and cyber security of North America's electricity systems."

Online

http://purl.access.gpo.gov/GPO/LPS25932

http://purl.access.gpo.gov/GPO/LPS25934 (PDF)

EMERGING THREATS: ASSESSING NUCLEAR WEAPONS COMPLEX FACILITY SECURITY. U.S. Congress. House. Committee on Government Reform. Subcommittee on National Security, Emerging Threats and International Relations. 108th Congress, 1st Session, 24 June 2003. Washington, DC: U.S. Government Printing Office, 2003. 187p. [Hearing].

SuDoc# Y 4. G 74/7: T 41/7

> "Even before the attacks of September 11, 2001 forced a reevaluation of physical security standards and procedures, serious questions arose concerning lax management and a stubborn cultural antipathy to protective measures at sites housing plutonium and highly enriched uranium. In response, Congress established the National Nuclear Security Administration [NNSA], as a semi-autonomous agency within the Department of Energy [DOE], to focus resources and high-level management attention on security mandates. However, creation of the NNSA failed to stem persistent reports of security lapses and inattentiveness to lingering vulnerabilities throughout the weapons complex … GAO has found a lack of clear roles and responsibilities among NNSA security offices, inconsistent assessments of contractor performance, potentially critical staff shortfalls and a failure to address the root causes of security lapses. As a result, neither the Department of Energy nor the NNSA can yet provide reasonable assurance weapons grade material is protected against a determined, well-trained adversarial force willing to die in a nuclear detonation or radiological dispersion of their own making."

Online

http://purl.access.gpo.gov/GPO/LPS42910 (PDF)

EMERGING THREATS: ASSESSING PUBLIC SAFETY AND SECURITY MEASURES AT NUCLEAR POWER FACILITIES. U.S. Congress. House. Committee on Government Reform. Subcommittee on National Security, Emerging Threats and International Relations. 108th Congress, 1st Session, 10 March 2003. Washington, DC: U.S. Government Printing Office, 2003. 322p. [Hearing].

SuDoc# Y 4. G 74/7: T 41/5

> "Today, we ask if Federal regulators are demanding the physical security and preparedness enhancements needed to protect public health and safety from nuclear terrorism. Recent reports suggest the answer may be no. Although specific to the Indian Point reactor complex in Buchanan, NY, observations by the General Accounting Office [GAO], and to a private security firm point to systemic weaknesses in nuclear incident response planning that have implications for every community within 50 miles of any of the Nation's 64 active reactor sites. A release of radiation

> caused by terrorists is a unique event, one that requires acknowledgment of the distinct factors and fears that will define the public response to such an incident. Yet the chairman of the Nuclear Regulatory Commission [NRC], recently wrote, 'Necessary protective actions and response are not predicated on the cause of events.'"

Online

http://purl.access.gpo.gov/GPO/LPS40095

http://purl.access.gpo.gov/GPO/LPS40096 (PDF)

THE ENCRYPTION DEBATE: CRIMINALS, TERRORISTS, AND THE SECURITY NEEDS OF BUSINESS AND INDUSTRY. U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Technology, Terrorism, and Government Information. 105th Congress, 1998. Washington, DC: U.S. Government Printing Office, 1998. 116p. [Hearing].

SuDoc# Y 4. J 89/2: S.HRG.105-415

> "The law enforcement community locally, nationally, and abroad is extremely concerned about the serious threat posed by the use of encryption by violent criminals, terrorists, child pornographers, drug traffickers … our Government has long used encryption to protect vital government information systems. In an era of information warfare, protecting the Nation's critical infrastructures against terrorists and other threats will require the strategic use of encryption and other protective measures."

ENCRYPTION SECURITY IN A HIGH TECH ERA. U.S. Congress. House. Committee on International Relations. Subcommittee on International Economic Policy and Trade. 106th Congress, 1st Session, 18 May 1999. Washington, DC: U.S. Government Printing Office, 2000. 60p. [Hearing].

SuDoc# Y 4. IN 8/16: SE 2/9

> As sensitive and private electronic information transfers become more common, "fear has emerged about their security and about the interception of messages and transactions by those who seek to steal or sabotage."

Online

http://purl.access.gpo.gov/GPO/LPS5037

http://purl.access.gpo.gov/GPO/LPS5038 (PDF)

ENHANCING COMPUTER SECURITY: WHAT TOOLS WORK BEST. U.S. Congress. House. Committee on Government Reform. Subcommittee on Government Management, Information, and Technology. 106th Congress, 2nd Session, 29 March 2000. Washington, DC: U.S. Government Printing Office, 2001. 84p. [Hearing].

SuDoc# Y 4. G 74/7: C 73/37

> “Electronic government and electronic commerce trends should continue to dictate the way important data are exchanged. From tax refunds and health records to credit card purchases and Social Security numbers, organizations must demonstrate that the information flowing into their computers is secure. Tools are available to help organizations and citizens protect their computers against unwanted and unruly intruders. However, they must be carefully used to ensure that they lead to meaningful improvement.”

Online

http://purl.access.gpo.gov/GPO/LPS10473

http://purl.access.gpo.gov/GPO/LPS10474 (PDF)

ENSURING THE SAFETY OF OUR FEDERAL WORKFORCE: GSA’s USE OF TECHNOLOGY TO SECURE FEDERAL BUILDINGS. U.S. Congress. House. Committee on Government Reform. Subcommittee on Technology and Procurement Policy. 107th Congress, 2nd Session, 25 April 2002. Washington, DC: U.S. Government Printing Office, 2003. 83p. [Hearing].

SuDoc# Y 4. G 74/7: W 89/12

> “The terrorist attacks of September 11th have led to a renewed assessment of the vulnerability of Federal buildings and focus on a new array of security threats. The acquisition of technological upgrades and new technologies are part of the broader effort to combat these threats. And the effective use of these technologies will be critical to our success. Today, we are going to examine what role technology plays in the security initiatives that GSA is currently implementing in order to protect Federal buildings and the employees who work in them. We will also try to ascertain what barriers may exist in obtaining and implementing the most appropriate and effective technologies.”

Online

http://purl.access.gpo.gov/GPO/LPS30751 (PDF)

EXAMINING SECURITY AT FEDERAL FACILITIES: ARE ATLANTA’S FEDERAL EMPLOYEES AT RISK? U.S. Congress. House. Committee on Government Reform. 107th Congress, 2nd Session, 30 April 2002. Washington, DC: U.S. Government Printing Office, 2002. 83p. [Hearing].

SuDoc# Y 4. G 74/7: SE 2/24

> “Today representatives from the General Accounting Office, Office of Special Investigations [OS I], will provide testimony on the results of a recently completed investigation … Acting in an undercover capacity investigators were able to gain

> unauthorized access to these buildings, they gained access which allowed them unfettered admission to any areas of the buildings day or night … By employing a few simple tactics and off-the-shelf technology investigators thwarted the security in such a manner that weapons, explosives, nuclear, chemical, or biological agents, listening devices, and other life-threatening or hazardous materials could have easily been carried into and left throughout these Federal buildings."

Online

http://purl.access.gpo.gov/GPO/LPS23530 (PDF)

FAA's CIVIL AVIATION SECURITY PROGRAM. U.S. Congress. House. Committee on Government Operations. Subcommittee on Government Activities and Transportation. 99th Congress, 1st Session, 27 June 1985. Washington, DC: U.S. Government Printing Office, 1985. 36p. [Hearing].

SuDoc# Y 4. G 74/7: AV 5/6

> "Americans are enraged at the hijacking of the TWA 727, the murder of a U.S. serviceman, and the holding hostage of its passengers. Next came the bombing of Frankfurt's airport, and suddenly, in rapid succession, the suspected sabotage of an Air India 747, killing 329 people near the coast of Ireland, of the bomb explosion in a baggage container at Tokyo's Narita Airport. Each of these incidents tragically demonstrates the vulnerability of air passengers, flight crews, airport employees and the public at large to the murderous schemes of terrorists. They also point out that aviation security encompasses not only passenger and baggage screening at airports, but extends beyond their physical boundaries."

FBI COMPUTERS: 1992 HARDWARE—2002 PROBLEMS. U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Administrative Oversight and the Courts. 107th Congress, 2nd Session, 16 July 2002. Washington, DC: U.S. Government Printing Office, 2003. 46p. [Hearing].

SuDoc# Y 4. J 89/2: S.HRG.107-989

> "We all agree on the problems with the FBI's technology infrastructure have taken on a new urgency since September 11. But these problems, as we know, have been around for a long time … For a long time, the FBI's data base warehouse was like Medusa, with over 40 data bases with separate functions operating out of the same body but totally disconnected from one another … Dinosaur-era technology, like the painstaking process it takes for an agent to use the automated case system where an FBI agent has to make her way through 12 different functions just to store a document must be transformed into efficient, accessible, streamlined technology. Another example of a fossil technology is the FBI's inability to search across different data bases by plugging in a couple of key words … 'DOJ concluded that the FBI's

troubled information systems are likely to have a continuing negative impact on its ability to properly investigate crimes and analyze information throughout the FBI.'"

Online

http://purl.access.gpo.gov/GPO/LPS41016 (PDF)

FEDERAL BUILDING SECURITY. U.S. Congress. House. Committee on Transportation and Infrastructure. Subcommittee on Public Buildings and Economic Development. 104th Congress, 2nd Session, 4 April; 24 May 1996. Washington, DC: U.S. Government Printing Office, 1997. 94p. [Hearing].

SuDoc# Y 4. T 68/2: 104-70

Examines federal building security plan changes and implementation one year after the Murrah Federal Building bombing in Oklahoma City.

FINAL REPORT TO PRESIDENT CLINTON: WHITE HOUSE COMMISSION ON AVIATION SAFETY AND SECURITY. Office of the President (William J. Clinton). 12 February 1997. Washington, DC: White House Commission on Aviation Safety and Security, 1997. 88p. [Report].

SuDoc# PR 42.8: AV 5

"…the roles of intelligence and law enforcement agencies in supporting the FAA must be more clearly defined and coordinated. The terrorist threat is changing and growing. Therefore, it is important to improve security not just against familiar threats, such as explosives in checked baggage, but also to explore means of assessing and countering emerging threats, such as the use of biological or chemical agents, or the use of missiles."

Online

http://purl.access.gpo.gov/GPO/LPS19581

http://permanent.access.gpo.gov/lps19581/whc97rpt.htm

FOOD-PROCESSING SECURITY: VOLUNTARY EFFORTS ARE UNDER WAY, BUT FEDERAL AGENCIES CANNOT FULLY ASSESS THEIR IMPLEMENTATION. U.S. General Accounting Office. February 2003. Washington, DC: U.S. General Accounting Office, 2003. 47p. [Report].

SuDoc# GA 1.13: GAO-03-342

"This report recommends that the Secretaries of the Departments of Health and Human Services and Agriculture study their agencies' existing statutes to identify what additional authorities they may need relating to security measures at food-processing facilities to reduce the risk of deliberate contamination of the food supply.

On the basis of these studies' results, the agencies should seek additional authority from the Congress, as needed. GAO also recommends that the agencies provide training for all food inspection personnel to enhance their awareness and ability to discuss security measures with plant personnel. USDA agreed with this report's recommendations. FDA agreed with the recommendation to provide training for all food inspection personnel but took no position on GAO's other recommendation."

Online

http://www.gao.gov/new.items/d03342.pdf (PDF)

FOOD SAFETY: AGENCIES SHOULD FURTHER TEST PLANS FOR RESPONDING TO DELIBERATE CONTAMINATION. U.S. General Accounting Office. October 1999. Washington, DC: U.S. General Accounting Office, 1999. 10p. [Report].

SuDoc# GA 1.13: RCED-00-3

GAO was asked to "(1) determine the extent to which food has been deliberately contaminated with a biological agent (bacteria, virus, or toxin) or threatened to be contaminated with such an agent and (2) describe the plans and procedures that federal food safety regulatory agencies have for responding to threats and acts of deliberate food contamination with a biological agent."

Online

http://www.gao.gov/docdblite/summary.php?recflag=&accno=163034&rptno=RCED-00-3
(Abstract Only)

http://www.mipt.org/pdf/gaorced003.pdf (PDF)

FOOD SAFETY AND SECURITY: CAN OUR FRACTURED FOOD SAFETY SYSTEM RISE TO THE CHALLENGE? U.S. Congress. Senate. Committee on Governmental Affairs. Subcommittee on Oversight of Government Management, Restructuring, and the District of Columbia. 2002. 155p. [Hearing].

SuDoc# Y 4. G 74/9: S.HRG.107-210

"Following the events of September 11, we are more keenly focused on how varied aspects of America's homeland security, including our Nation's food supply, may be vulnerable to attack. Our Federal food safety system must be able to prevent potential food hazards from reaching the public."

Online

http://purl.access.gpo.gov/GPO/LPS22832 (PDF)

HOMELAND SECURITY: FINDING THE NUCLEAR NEEDLE IN THE CARGO CONTAINER HAYSTACK. U.S. Congress. House. Committee on Government Reform. Subcommittee on

National Security, Veterans Affairs and International Relations. 107th Congress, 2nd Session, 18 November 2002. Washington, DC: U.S. Government Printing Office, 2003. 159p. [Hearing].

SuDoc# Y 4. G 74/7: H 75/17

> "Ubiquitous cargo containers are of particular concern. An estimated 11million containers worldwide are each loaded and unloaded 10 times per year. 21,000 containers arrive at U.S. ports each day. Each trip by a cargo container represents a potential vector of stealth attack. No security standards govern container transport. A recent event … underscored the peril posed by containerized nuclear cargo. 15 pounds of depleted uranium arrived here undetected."

Online

http://purl.access.gpo.gov/GPO/LPS34419 (PDF)

HOMELAND SECURITY: PROTECTING AIRLINERS FROM TERRORIST MISSILES. Library of Congress. Christopher Bolkcom and Bartholomew Elias. 3 November 2003. Washington, DC: Congressional Research Service, Library of Congress, 2003. 18p. [Online Report].

SuDoc# LC 14.19/3: RL31741

> "Recent events have focused attention on the threat that terrorists with shoulder fired surface-to-air missiles (SAMs) pose to commercial airliners. Most believe that no single solution exists to effectively mitigate this threat. Instead, a menu of options may be considered, including installing infrared (IR) countermeasures on aircraft; modifying flight operations and air traffic control procedures; improving airport and regional security; and strengthening missile non-proliferation efforts."

Online

http://www.fas.org/irp/crs/RL31741.pdf (PDF)

HOMELAND SECURITY: PROTECTING STRATEGIC PORTS. U.S. Congress. House. Committee on Government Reform. Subcommittee on National Security, Veterans Affairs and International Relations. 107th Congress, 2nd Session, 5 August 2002. Washington, DC: U.S. Government Printing Office, 2003. 205p. [Hearing].

SuDoc# Y 4. G 74/7: H 75/15

> "A qualitative not a quantitative approach is required to improve port security. Various estimates about the tiny fraction of imports actually inspected could be reassuring, not frightening, if we could be sure that the right ships and warehouses were being inspected, those posing the most risk. Knowing that is a matter of intelligence at ports of origin, of diligence in the search for anomalies in a sea of routine trade data, and a vigilance in engaging high-risk cargoes before they reach the dockside. Tension between tighter security and faster commerce is inevitable."

Online

http://purl.access.gpo.gov/GPO/LPS34401 (PDF)

HOMELAND SECURITY: SECURING STRATEGIC PORTS. U.S. Congress. House. Committee on Government Reform. Subcommittee on National Security, Veterans Affairs and International Relations. 107th Congress, 2nd Session, 23 July 2002. Washington, DC: U.S. Government Printing Office, 2003. 82p. [Hearing].

SuDoc# Y 4. G 74/7: H 75/16

> "The detonation of a ship-based weapon of mass destruction would have disastrous effects on our military and our economy. This is a nightmare we cannot allow. How are we going to prevent this scenario? Specifically, how are we going to keep these very lethal threats from endangering our ports of embarkation and military bases?"

Online

http://purl.access.gpo.gov/GPO/LPS34463 (PDF)

HOMELAND SECURITY: THE FEDERAL AND NEW YORK RESPONSE. U.S. Congress. House. Committee on Science. 107th Congress, 2nd Session, 24 June 2002. Washington, DC: U.S. Government Printing Office, 2003. 100p. [Hearing].

SuDoc# Y 4. SCI 2: 107-71

> "…the third in a series of hearings examining the vulnerability of our nation's computer infrastructure as well as research and education challenges and opportunities facing the Nation's network security infrastructure and management. The Committee will also examine the connections between the Nation's science and technology enterprise and U.S. law enforcement and other first responders in the fight against cyber terrorism."

HOMELAND SECURITY: VOLUNTARY INITIATIVES ARE UNDER WAY AT CHEMICAL FACILITIES BUT THE EXTENT OF SECURITY PREPAREDNESS IS UNKNOWN. U.S. General Accounting Office. March 2003. Washington, DC: U.S. General Accounting Office, 2003. [Report].

SuDoc# GA 1.13: GAO-03-439

> "To its credit, the chemical industry, led by its industry associations, has undertaken a number of voluntary initiative to address security at facilities. For example, the American Chemistry Council, whose members own or operate 1,000, or 7 percent, of the facilities subject to Clean Air Act risk management plan provisions, requires its members to conduct vulnerability assessments and implement security improvements. The industry faces a number of challenges in preparing facilities against attacks, including ensuring that all chemical facilities address security concerns. Despite the

> industry's voluntary efforts, the extent of security preparedness at U.S. chemical facilities is unknown. Finally, both the Secretary of Homeland Security and the Administrator of EPA have stated that voluntary efforts alone are not sufficient to assure the public of industry's preparedness."

Online

http://purl.access.gpo.gov/GPO/LPS32264 (PDF)

http://www.gao.gov/new.items/d03439.pdf (PDF)

HOW SECURE IS OUR CRITICAL INFRASTRUCTURE? U.S. Congress. Senate. Committee on Governmental Affairs. 107th Congress, 1st Session, 12 September 2001. Washington, DC: U.S. Government Printing Office, 2002. 87p. [Hearing].

SuDoc# Y 4. G 74/9: S.HRG.107-205

> "Today, individuals or terrorists or nations with no chance of success against America on the battlefield can pose just as significant a threat to our society from the isolation of their homes or offices or terrorist camps. The nature of our critical infrastructure has changed that much in the information age."

IMPACT ABROAD OF THE ACCIDENT AT THE THREE MILE ISLAND NUCLEAR POWER PLANT: MARCH-SEPTEMBER **1979***.* U.S. Congress. Senate. Committee on Governmental Affairs. Subcommittee on Energy, Nuclear Proliferation and Federal Services. 96th Congress, 1st Session, 5 July; 19 October 1979; 13 February 1980. Washington, DC: U.S. Government Printing Office, 1980. 81p. [Hearing].

SuDoc# Y 4. G 74/9: N 88/10

> "On March 28, 1979, an accident occurred in a nuclear power plant at Three Mile Island, near Harrisburg, Pennsylvania. It caused widespread fears of catastrophe and raised doubts as to the adequacy of what some nuclear utilities and the U.S. Nuclear Regulatory Commission have done to assure safe operation of nuclear power plants."

IMPROVING OUR ABILITY TO FIGHT CYBERCRIME: OVERSIGHT OF THE NATIONAL INFRASTRUCTURE PROTECTION CENTER. U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Technology, Terrorism, and Government Information. 107th Congress, 1st Session, 25 July 2001. Washington, DC: U.S. Government Printing Office, 2002. 81p. [Hearing].

SuDoc# Y 4. J 89/2: S.HRG.107-366

> "The cyber war being waged against America's infrastructure is not limited to hackers seeking the thrill of the game of disrupting computer systems. It is being waged as well by criminal groups, by foreign intelligence services, insider threats from disgruntled employees, and even politically motivated groups…It is a frightening

> thought to imagine the damage that could be done if someone gained control of systems that serve our communications, financial, transportation, electrical, or defense systems in our country."

Online

http://purl.access.gpo.gov/GPO/LPS19294

http://purl.access.gpo.gov/GPO/LPS19295 (PDF)

IMPROVING SECURITY AND FACILITATING COMMERCE AT THE NATION'S PORTS OF ENTRY: SEAPORTS OF LOS ANGELES AND LONG BEACH, CA. U.S. Congress. House. Committee on Government Reform. Subcommittee on Criminal Justice, Drug Policy and Human Resources. 107th Congress, 2nd Session, 1 February 2002. Washington, DC: U.S. Government Printing Office, 2003. 122p. [Hearing].

SuDoc# Y 4. G 74/7: SE 2/27

> "Simply stated, the Los Angeles—Long Beach complex is the nation's Superport. Individually, the port of Los Angeles or the Port of Long Beach would rank as the largest cargo port in the United States. As a complex, Los Angeles—Long Beach represents the third largest port in the world, handling over 35% of the nation's containerized cargo, over 1 million cruise passengers and over 50% of the petroleum products used in the western United States…On 11 September, immediate actions were necessary to ensure heightened security…"

Online

http://purl.access.gpo.gov/GPO/LPS32997 (PDF)

INFORMATION CONCERNING THE ARMING OF COMMERCIAL PILOTS. U.S. General Accounting Office. Gerald L. Dillingham. 28 June 2002. Washington, DC: U.S. General Accounting Office, 2002. 13p. [Report].

SuDoc# GA 1.13: GAO-02-822 R

"Without additional research, the potential benefits, risks, and costs of using weapons on aircraft cannot be fully determined. Proponents' and opponents' views on allowing pilots to carry firearms in the cockpit fell into four categories: the potential effectiveness, risk, and cost-effectiveness of their carrying weapons, and the policy issues that would arise if pilots were allowed to carry weapons … Views also differed on whether arming pilots with firearms would be effective or safe … Finally, views differed on the public policy implications of arming pilots."

Online

http://purl.access.gpo.gov/GPO/LPS34809 (PDF)

http://www.gao.gov/new.items/d02822r.pdf (PDF)

INFORMATION SECURITY: CONTINUED EFFORTS NEEDED TO FULLY IMPLEMENT STATUTORY REQUIREMENTS: STATEMENT OF ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY ISSUES. U.S. General Accounting Office. 24 June 2003. Washington, DC: U.S. General Accounting Office, 2003. 36p. [Testimony].

SuDoc# GA 1.5/2: GAO-03-852 T

> "Based on the fiscal year 2002 reports submitted to OMB, the federal government has made limited overall progress in implementing statutory information security requirements, although a number of benefits have resulted. Among these benefits are several actions taken and planned to address governmentwide information security weaknesses and challenges, such as a lack of senior management attention. Nevertheless, as indicated by selected quantitative performance measures for the largest federal agencies, progress has been limited. Specifically, excluding data for one agency that were not comparable for fiscal years 2001 and 2002, improvements for 23 agencies ranged from 3 to 10 percentage points for the selected measures."

Online

http://www.gao.gov/cgi-bin/getrpt?GAO-03-852T (PDF)

http://www.gao.gov/new.items/d03852t.pdf (PDF)

INFORMATION SECURITY: CORPS OF ENGINEERS MAKING IMPROVEMENTS, BUT WEAKNESSES CONTINUE—REPORT TO THE COMMANDING GENERAL, U.S. ARMY COPRS OF ENGINEERS. U.S. General Accounting Office. 10 June 2002. Washington, DC: U.S. General Accounting Office, 2002. 24p. [Report].

SuDoc# GA 1.13: GAO-02-589

> "…continuing and newly identified vulnerabilities involving general and application computer controls continue to impair the Corps' ability to ensure the reliability, confidentiality, and availability of financial and sensitive data. These vulnerabilities warrant management's attention to decrease the risk of inappropriate disclosure and modification of data and programs, misuse or damage to computer resources, or disruption of critical operations. Such vulnerabilities also increase risks to other Department of Defense (DOD) networks and systems to which the Corps' network is linked."

Online

http://purl.access.gpo.gov/GPO/LPS34922

INFORMATION SECURITY: PROGRESS MADE BUT CHALLENGES REMAIN TO PROTECT FEDERAL SYSTEMS AND THE NATION'S CRITICAL INFRASTRUCTURES: STATEMENT OF ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY ISSUES. U.S. General

Accounting Office. 8 April 2003. Washington, DC: U.S. General Accounting Office, 2003. [Testimony].

SuDoc# GA 1.5/2: GAO-03-654 T

> "Although improvements have been made in protecting our nation's critical infrastructures and continuing efforts are in progress, further efforts are needed to address critical challenges that GAO has identified over the last several years. These challenges include: developing a comprehensive and coordinated CIP plan; improving information sharing on threats and vulnerabilities between the private sector and the federal government, as well as within the government itself; improving analysis and warning capabilities for both cyber and physical threats; and encouraging entities outside the federal government to increase their CIP efforts."

Online

http://purl.access.gpo.gov/GPO/LPS36535 (PDF)

http://www.gao.gov/cgi-bin/getrpt?GAO-03-564T (PDF)

http://www.gao.gov/new.items/d03564t.pdf (PDF)

INFORMATION SECURITY: SUBCOMMITTEE POST-HEARING QUESTIONS CONCERNING THE ADDITIONAL ACTIONS NEEDED TO IMPLEMENT REFORM LEGISLATION. U.S. General Accounting Office. 16 April 2002. Washington, DC: U.S. General Accounting Office, 2002. 5p. [Questions].

SuDoc# GA 1.13: GAO-02-649 R

> "We agree that the six security weaknesses OMB identified in its report to the Congress represent significant deficiencies in federal departments' and agencies' information security programs. Specifically, these are (1) a lack of senior management attention to information security; (2) inadequate accountability for job and program performance related to information technology security; (3) limited security training for general users, information technology professionals, and security professionals; (4) inadequate integration of security into the capital planning and investment control process; (5) poor security for contractor-provided services; and (6) limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections."

Online

http://purl.access.gpo.gov/GPO/LPS38575 (PDF)

http://www.gao.gov/new.items/d02649r.pdf (PDF)

INFORMATION TECHNOLOGY—ESSENTIAL YET VULNERABLE: HOW PREPARED ARE WE FOR ATTACKS? U.S. Congress. House. Committee on Government Reform. Subcommittee on Government Efficiency, Financial Management and Intergovernmental

Relations. 107th Congress, 1st Session, 26 September 2001. Washington, DC: U.S. Government Printing Office, 2002. 180p. [Hearing].

SuDoc# Y 4. G 74/7: T 22/10

> "…imagine the repercussions if attacks on the Federal Government's critical computers were … successful. National defense, communications, transportation, public health, and emergency response services across the Nation could be crippled instantly … In addition to the threat of physical assault, the Nation's information technology systems are already under cyber-assault … Is the Nation ready for this type of terrorism? Will its basic communications and computer infrastructure withstand a major assault?"

Online

http://purl.access.gpo.gov/GPO/LPS22473

http://purl.access.gpo.gov/GPO/LPS22474 (PDF)

INFORMATION TECHNOLOGY: HOMELAND SECURITY NEEDS TO IMPROVE ENTRY EXIT SYSTEM EXPENDITURE PLANNING. U.S. General Accounting Office. June 2003. Washington, DC: U.S. General Accounting Office, 2003. [Report].

SuDoc# GA 1.13: GAO-03-563

> "GAO observed that INS has preliminary plans showing that it intends to acquire and deploy a system that has functional and performance capabilities that satisfy the general scope of capabilities required under various laws. These include the capability to (1) collect and match alien arrival and departure data electronically; (2) be accessible to the border management community (including consular officers, federal inspection agents, and law enforcement and intelligence agencies responsible for identifying and investigating foreign nationals); and (3) support machine-readable, tamper-resistant documents with biometric identifiers at ports of entry. Each of these capabilities is integral to supporting our nation's border security process."

Online

http://www.gao.gov/cgi-bin/getrpt?GAO-03-563 (PDF)

http://www.gao.gov/new.items/d03563.pdf (PDF)

INFORMATION TECHNOLOGY: INS NEEDS TO STRENGTHEN ITS INVESTMENT MANAGEMENT CAPABILITY. U.S. General Accounting Office. December 2000. Washington, DC: U.S. General Accounting Office, 2000. 64p. [Report].

SuDoc# GA 1.13: GAO-01-146

> "INS obligated about $18 million in fiscal year 2000 to further deploy its Integrated Surveillance Intelligence System (ISIS), which includes the deployment of intelligent

> computer aided detection systems, unattended ground sensors, and fixed cameras along the northern and southern borders to provide around-the-clock visual coverage of the border."

Online

http://purl.access.gpo.gov/GPO/LPS9577 (PDF)

INTERNET SECURITY. U.S. Congress. Senate. Committee on Commerce, Science, and Transportation. Subcommittee on Communications. 106th Congress, 2nd Session, 8 March 2000. Washington, DC: U.S. Government Printing Office, 2003. 64p. [Hearing].

SuDoc# Y 4. C 73/7: S.HRG.106-1092

> "And this is not just a crime problem. It is also a national security problem. That is because our Nation's critical infrastructures—including things such as telecommunications, electrical energy, and banking and finance, those things that are vital to our national security as well as our national economy—are all dependent on computer technology. But that very dependence makes them vulnerable to sorts of attacks that did not exist 10 or 15 years ago."

Online

http://purl.access.gpo.gov/GPO/LPS33951

http://purl.access.gpo.gov/GPO/LPS33952 (PDF)

LAND BORDER PORTS OF ENTRY: VULNERABILITIES AND INEFFICIENCIES IN THE INSPECTIONS PROCESS. U.S. General Accounting Office. 18 August 2003. Washington, DC: U.S. General Accounting Office, 2003. [Report].

SuDoc# GA 1.41: GAO-03-1084 R

> "Our observations and interviews at 15 land border POEs identified several vulnerabilities in the integrity of the inspections process, which raise the risk of unlawful entry. For example, inspectors can experience difficulties in verifying the identity of travelers, travel inspections were not always done consistently and according to policy, and inspectors did not always receive the training they needed."

Online

http://purl.access.gpo.gov/GPO/LPS37835 (PDF)

http://www.gao.gov/cgi-bin/getrpt?GAO-03-1084R (PDF)

http://www.gao.gov/new.items/d031084r.pdf (PDF)

MAKING FEDERAL COMPUTERS SECURE: OVERSEEING EFFECTIVE INFORMATION SECURITY MANAGEMENT. U.S. Congress. House. Committee on Government Reform. 107th

Congress, 2nd Session, 24 October 2002. Washington, DC: U.S. Government Printing Office, 2002. 20p. [Report].

SuDoc# Y 1.1/8: 107-764

> "Federal agencies rely extensively on computerized systems and electronic data to support operations that are essential to the health and well being of all Americans. Critical Government systems, from national defense and emergency services to tax collection and benefit payments, rely on electronically stored information and automated systems. Maintaining adequate security over these systems and the electronic data stored in them is essential to maintaining the continuity of the Government's critical operations. Security measures must prevent data tampering, fraud, sabotage and the inappropriate disclosure of sensitive information. Nevertheless, independent audits and evaluations continue to show that most Federal departments and agencies have pervasive weaknesses in their computer security programs that pose serious risks to these critical automated systems."

Online

http://purl.access.gpo.gov/GPO/LPS25073 (PDF)

THE NATION AT RISK: REPORT OF THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION. U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Technology, Terrorism, and Government Information. 105th Congress, 1st Session, 5 November 1997. Washington, DC: U.S. Government Printing Office, 1998. 72p. [Hearing].

SuDoc# Y 4. J 89/2: S.HRG.105-447

> "It is far from clear that the Department of Defense has the means or authority to prepare peacetime defenses to detect or assess an information warfare attack, or to direct and supply active defenses during an attack. But one thing is clear—key national security assets are not within the range, power, or current responsibility of the armed forces to protect in the traditional manner in which they would have defended the Nation against conventional attack in World War II or nuclear attack during the cold war."

THE NATIONAL STRATEGY TO SECURE CYBERSPACE. Office of the President (George W. Bush). February 2003. Washington, DC: U.S. Department of Homeland Security, 2003. 60p. [Report].

SuDoc# PR 43.8: IN 3/2003

> "The policy of the United States is to protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States. We must act to reduce our vulnerabilities to these threats before they can be exploited to damage

> the cyber systems supporting our Nation's critical infrastructures and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible."

Online

http://purl.access.gpo.gov/GPO/LPS28730 (PDF)

http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf (PDF)

NUCLEAR INFRASTRUCTURE SECURITY ACT. U.S. Congress. Senate. Committee on Environment and Public Works. 108th Congress, 1st Session, 6 November 2003. Washington, DC: U.S. Government Printing Office, 2003. 73p. [Report].

SuDoc# Y 1.1/5: 108-190

> "The Nuclear Infrastructure Security Act of 2003 (NISA) is an important step is ensuring protection of the public against potential terrorist activities against commercial nuclear facilities or potential theft of nuclear materials. While the NRC [Nuclear Regulatory Commission] has voluntarily undertaken a number of actions, these have been ad hoc responses to emergency events. The purpose of this legislation is to codify those actions necessary to protect against attack on our nation's nuclear reactors and against theft or terrorist use of radioactive materials, such as for so-called 'dirty bombs.' The legislation gives clear and permanent direction to the NRC and its licensees, and DHS [Department of Homeland Security]. NISA will assure the American public that these nuclear facilities are as safe as they can reasonably be, and will clearly signal to would-be terrorists that our nuclear facilities are heavily protected, hardened structures that will make neither easy, nor desirable, targets."

bombs.' The legislation gives clear and permanent direction to the NRC and its licensees, and DHS [Department of Homeland Security]. NISA will assure the American public that these nuclear facilities are as safe as they can reasonably be, and will clearly signal to would-be terrorists that our nuclear facilities are heavily protected, hardened structures that will make neither easy, nor desirable, targets."

Online

http://purl.access.gpo.gov/GPO/LPS41336

http://purl.access.gpo.gov/GPO/LPS41337 (PDF)

NUCLEAR REACTOR SAFETY. U.S. Congress. House. Committee on Energy and Commerce. Subcommittee on Energy Conservation and Power. 99th Congress, 2nd Session, 22 May; 16 July 1986. Washington, DC: U.S. Government Printing Office, 1987. 566p. [Hearing].

SuDoc# Y 4. EN 2/3: 99-177

> "The nuclear industry has not achieved uniform standards of excellence. Some plants have state-of-the-art technology. Some are well-managed. Some are appropriately

> located in areas away from population centers. Some are efficient, cost-effective producers of electricity. A few—those run by the military—have adequate security. However, many others were poorly designed and now have outdated equipment. They are located in areas that are densely populated or are vulnerable because of their geography…Nearly all civilian reactors have inadequate protection from new and more sophisticated security threats."

NUCLEAR SECURITY: DOE NEEDS TO IMPROVE CONTROL OVER CLASSIFIED INFORMATION. U.S. General Accounting Office. August 2001. Washington, DC: U.S. General Accounting Office, 2001. 27p. [Report].

SuDoc# GA 1.13: GAO-01-806

> "…DOE does not have requirements for documenting need-to-know determinations. Without such requirements, the justification for granting need to know was not documented in many cases and DOE cannot ensure that access to classified information is limited only to individuals who have appropriate clearances and whose work requires access to specific classified information for a specific period of time."

Online

http://www.fas.org/sgp/othergov/doe/gao01806.pdf (PDF)

OVERSIGHT HEARING ON AVIATION SECURITY. U.S. Congress. Senate. Committee on Commerce, Science, and Transportation. Subcommittee on Aviation. 106th Congress, 2nd Session, 6 April 2000. Washington, DC: U.S. Government Printing Office, 2003. 66p. [Hearing].

SuDoc# Y 4. C 73/7: S.HRG.106-1136

> "In terms of the actual screening of passengers, the pre-boarding security screeners are a Maginot line between safety and those with ill intent. Although they are hard working and often dedicated, the turnover rate at most airports is over 100%. At one airport in particular, it was recently over 400%. A seasoned screener pool is essential to effective screening. However, nowadays it is very difficult to find a screener with more than a couple of months of experience at these airports. Consequently, the Department of Transportation Inspector General's Office (DOT IG) and the General Accounting Office (GAO) have expressed concerns about screener performance."

Online

http://purl.access.gpo.gov/GPO/LPS39396 (PDF)

OVERSIGHT OF THE U.S. POSTAL SERVICE: ENSURING THE SAFETY OF POSTAL EMPLOYEES AND THE U.S. MAIL. U.S. Congress. House. Committee on Government

Reform. 107th Congress, 1st Session, 30 October 2001. Washington, DC: U.S. Government Printing Office, 2002. 187p. [Hearing].

SuDoc# Y 4. G 74/7: P 84/29

> "Our mail system is vital to the Nation, accounting for approximately 8 percent of the gross national product. The overall goal of the Postal Service is to bind the Nation together through a communication system that is the best in the world … The perpetrators of anthrax-tainted mail seek to disrupt our communications network and threaten the viability of not only our mail service but of our Nation…"

Online

http://purl.access.gpo.gov/GPO/LPS21626

http://purl.access.gpo.gov/GPO/LPS21627 (PDF)

PORT SECURITY. U.S. Congress. House. Committee on Transportation and Infrastructure. Subcommittee on Coast Guard and Maritime Transportation. 107th Congress, 2nd Session, 6 December 2001; 13 February; 13 & 14 March 2002. Washington, DC: U.S. Government Printing Office, 2003. 351p. [Hearing].

SuDoc# Y 4. T 68/2: 107-57

> "Immediately following the events of September 11th, the Coast Guard launched the largest homeland port security operation since World War II. As part of Operation Noble Eagle and Operation Enduring Freedom, the Coast Guard established port and coastline patrols with 55 cutters, 42 aircraft and hundreds of small boats. Over 2,800 Coast Guard reservists were called to active duty to support maritime homeland security operations in 350 ports."

PORT SECURITY. U.S. Congress. Senate. Committee on Appropriations. Subcommittee on Transportation and Related Agencies. 107th Congress, 2nd Session, 4 April 2002. Washington, DC: U.S. Government Printing Office, 2002. 74p. [Special Hearing].

SuDoc# Y 4. AP 6/2: S.HRG.107-593

> "The greatest challenges we face are the potential threats posed by vessel crews, passengers and dangerous cargo. Containerization poses a major threat for smuggling drugs, terrorists and potentially weapons of mass destruction."

Online

http://purl.access.gpo.gov/GPO/LPS24296

http://purl.access.gpo.gov/GPO/LPS24297 (PDF)

PORT SECURITY: SECURITY FORCE MANAGEMENT. U.S. Department of Transportation. Washington, DC: U.S. Department of Transportation, 1998. 29p. [Report].

SuDoc# TD 1.61: SE 2

> "Security is a function of access control. Access control denies access to the port, its cargo storage areas, its staging areas, its communications, its sources of electrical power, its buildings, its docks, and its vessels to anyone contemplating criminal activity. This activity includes pilferage or theft of cargo or port property and equipment, drug smuggling, the landing of stowaways or illegal aliens, and the sabotage of port facilities or disruption of activities. In order to deny such access, full-time security measures must be established and exercised. Controlling access *into* the port through gates and checkpoints is only the first step."

POTENTIAL TERRORIST ATTACKS: ADDITIONAL ACTIONS NEEDED TO BETTER PREPARE CRITICAL FINANCIAL MARKET PARTICIPANTS. U.S. General Accounting Office. February 2003. Washington, DC: U.S. General Accounting Office, 2003. [Report].

SuDoc# GA 1.13: GAO-03-251

> "The September 11 attacks severely disrupted U.S. financial markets, resulting in the longest closure of the stock markets since the 1930s and severe settlement difficulties in the government securities market. While exchange and clearing organization facilities were largely undamaged, critical broker-dealers and bank participants had facilities and telecommunications connections damaged or destroyed. These firms and infrastructure providers made heroic and sometimes ad hoc and innovative efforts to restore operations. However, the attacks revealed that many of these organizations' business continuity plans (BCP) had not been designed to address wide-scale events."

Online

http://purl.access.gpo.gov/GPO/LPS30700 (PDF)

POTENTIAL TERRORIST ATTACKS: ADDITIONAL ACTIONS NEEDED TO BETTER PREPARE CRITICAL FINANCIAL MARKET PARTICIPANTS. U.S. General Accounting Office. February 2003. Washington, DC: U.S. General Accounting Office, 2003. [Report].

SuDoc# GA 1.13: GAO-03-414

> "The financial regulators have begun to jointly develop recovery goals and business continuity practices for organizations important for clearing; however, regulators have not developed strategies and practices for exchanges, key broker-dealers, and banks to ensure that trading can resume in a timely manner in future disasters. Individually, SEC has reviewed exchange and clearing organization risk reduction efforts, but had not generally reviewed broker-dealers' efforts. The bank regulators that oversee the major banks had guidance on information security and business continuity and reported examining banks' risk reduction measures annually."

Online

http://purl.access.gpo.gov/GPO/LPS30703 (PDF)

http://www.gao.gov/new.items/d03414.pdf (PDF)

PRACTICES FOR SECURING CRITICAL INFORMATION ASSETS. Office of the President (William J. Clinton). January 2000. Washington, DC: Critical Infrastructure Assurance Office, 2000. Various paginations. [Manual].

SuDoc# PR 42.8: IN 3/C 86/2

> "This guide includes chapters on establishing a security policy, identifying critical assets and performing vulnerability assessments, understanding the tools and practices available to improve security, and developing an effective incident response capability…"

Online

http://purl.access.gpo.gov/GPO/LPS5099 (PDF)

PROTECTING AMERICA'S CRITICAL INFRASTRUCTURE: HOW SECURE ARE GOVERNMENT COMPUTER SYSTEMS? U.S. Congress. House. Committee on Energy and Commerce. Subcommittee on Oversight and Investigations. 107th Congress, 1st Session, 5 April 2001. Washington, DC: U.S. Government Printing Office, 2001. 230p. [Hearing].

SuDoc# Y 4. C 73/8: 107-13

> "Today, the subcommittee holds a hearing to assess the security of government computer systems. In particular, we will assess how well or how poorly they are protecting our most critical cyberinfrastructures and operations from the threat of disgruntled insiders, hackers, criminals, terrorists, and rogue nation-states. Over the past 2 years this committee has conducted extensive oversight of computer security at particular government agencies … Our reviews consistently have found poor computer security planning and management and a general lack of compliance with existing requirements of law and policy."

PROTECTING THE HOMELAND: THE PRESIDENT'S PROPOSAL FOR REORGANIZING OUR HOMELAND SECURITY INFRASTRUCTURE. U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Technology, Terrorism, and Government Information. 107th Congress, 2nd Session, 25 June 2002. Washington, DC: U.S. Government Printing Office, 2003. 132p. [Hearing].

SuDoc# Y 4. J 89/2: S.HRG.107-928

> "On its own, consolidation of the border and transportation functions is already a massive undertaking. Over 90 percent of all the people to be housed in the president's proposed Department of Homeland Security will be responsible for just these two

> functions. And nearly 65 percent of the department's budget will go to these tasks. If on top of that, the critical infrastructure protection tasks—which are functionally akin to transportation security—were also to be included, then much of what the president has proposed to consolidate will have been accounted for."

Online

http://purl.access.gpo.gov/GPO/LPS32046 (PDF)

PROTECTION OF DOMESTIC DEPARTMENT OF STATE OCCUPIED FACILITIES; CONGRATULATING ALEJANDRO TOLEDO ON HIS ELECTION TO THE PRESIDENCY OF PERU, ETC.; THE GOVERNMENT OF THE PRC SHOULD CEASE ITS PERSECUTION OF FALUN GONG PRACTITIONERS; TERRORIST KIDNAPPERS IN ECUADOR AND SUPPORTING EFFORTS BY THE U.S. TO COMBAT SUCH TERRORISM; EXPORT ADMINISTRATION ACT OF 2001; VIETNAM HUMAN RIGHTS ACT; CORAL REEF AND COASTAL MARINE CONSERVATION ACT OF 2001. U.S. Congress. House. Committee on International Relations. 107th Congress, 1st Session, 1 August 2001. Washington, DC: U.S. Government Printing Office, 2001. 413p. [Markup].

SuDoc# Y 4. IN 8/16: D 71/3

> Efforts to protect U.S. Department of State buildings against the threat of domestic terrorist attacks.

Online

http://purl.access.gpo.gov/GPO/LPS42890 (PDF)

http://wwwc.house.gov/international_relations/107/74409.pdf (PDF)

REPORT OF THE INTERAGENCY COMMISSION ON CRIME AND SECURITY IN U.S. SEAPORTS: ABSTRACT. Office of the President (William J. Clinton). Fall 2000. Washington, DC: Interagency Commission on Crime and Security in U.S. Seaports, 2000. 20p. [Report Abstract].

SuDoc# PR 42.8: C 86/2 SE 1/ABSTRA

> "There are no widely accepted standards or guidelines for physical, procedural, and personnel security for seaports, although some ports are making outstanding efforts to improve security. Control of access to the seaport or sensitive areas within the seaports is often lacking. Practices to restrict or control the access of vehicles to vessels, cargo receipt and delivery operations, and passenger processing operations at seaports are either not present or not consistently enforced, increasing the risk that violators could quickly remove cargo or contraband."

RESTRICTIONS ON GENERAL AVIATION FLYING IN CLASS B AIRSPACE. U.S. Congress. House. Committee on Transportation and Infrastructure. Subcommittee on Aviation. 107th

Congress, 1st Session, 17 October 2001. Washington, DC: U.S. Government Printing Office, 2002. 116p. [Hearing].

SuDoc# Y 4. T 68/2: 107-53

> "Today's hearing of the Aviation Subcommittee is addressing restrictions on general aviation flying in Class B airspace and some of the impacts of those restrictions … the purpose of today's hearing is to examine the specific damage that has been done to general aviation as a result of the September 11th attack and the subsequent action of our own government on the grounding of general aviation."

REVIEW OF THE NATION'S INFRASTRUCTURE SECURITY. U.S. Congress. Senate. Committee on Environment and Public Works. 107th Congress, 1st Session, 1 November 2001. Washington, DC: U.S. Government Printing Office, 2003. 49p. [Hearing].

SuDoc# Y 4. P 96/10: S.HRG.107-662

> "On ensuring the security, protection, and preservation of public works, utilities, and economic zones against terrorist attack … With regard to infrastructure … this is one of those things that the public is looking to all of us as public officials to bring greater elements of security to the potential targets. Whether that is our water systems, nuclear power plants, chemical facilities, natural gas pipelines, whatever the issues that could be specific vehicles for a terrorist attack, I think we are remiss if we do not make sure that we have in place the kinds of quality checks and balances to make sure that these are secure."

Online

http://purl.access.gpo.gov/GPO/LPS30972

http://purl.access.gpo.gov/GPO/LPS30973 (PDF)

RIDING THE RAILS: HOW SECURE IS OUR PASSENGER AND TRANSIT INFRASTRUCTURE? U.S. Congress. Senate. Committee on Governmental Affairs. 107th Congress, 1st Session, 13 December 2001. Washington, DC: U.S. Government Printing Office, 2002. 136p. [Hearing].

SuDoc# Y 4. G 74/9: S.HRG.107-311

> "Trains and the transit system can be targets of terrorists. They travel in a predictable path at predictable times. Every year, America's public transportation infrastructure … carries 9 billion passengers … Nine billion passengers use our transit system as compared to 700 million air travelers annually."

Online

http://purl.access.gpo.gov/GPO/LPS21055

http://purl.access.gpo.gov/GPO/LPS21056 (PDF)

SECURING OUR INFRASTRUCTURE: PRIVATE/PUBLIC INFORMATION SHARING. U.S. Congress. Senate. Committee on Governmental Affairs. 107th Congress, 2nd Session, 8 May 2002. Washington, DC: U.S. Government Printing Office, 2003. 229p. [Hearing].

SuDoc# Y 4. G 74/9: S.HRG.107-550

> "The interdependency and inter-connectivity of government and industry computer networks increase the risks associated with cyber terrorism and cyber crimes. Any security weakness has the potential of being exploited through the Internet to gain unauthorized access to one or more of the connected systems. Information sharing can help protect our national security and critical infrastructure."

Online

http://purl.access.gpo.gov/GPO/LPS27037 (PDF)

SECURING OUR PORTS AGAINST TERROR: TECHNOLOGY, RESOURCES, AND HOMELAND DEFENSE. U.S. Congress. Senate. Committee on the Judiciary. Subcommittee on Technology, Terrorism, and Government Information. 107th Congress, 2nd Session, 26 February 2002. Washington, DC: U.S. Government Printing Office, 2003. 79p. [Hearing].

SuDoc# Y 4. J 89/2: S.HRG.107-855

> "Our seaports today are extremely vulnerable to terrorism. Drug trafficking, alien smuggling, export of stolen automobiles, and international cargo theft are rampant. Yet in spite of the fact that the major problems besetting seaports all fall within the traditional jurisdiction of United States law enforcement, no Federal agency currently has comprehensive authority to regulate activity at seaports."

Online

http://purl.access.gpo.gov/GPO/LPS29073 (PDF)

SECURITY IN FEDERAL BUILDINGS. U.S. Congress. House. Committee on Transportation and Infrastructure. Subcommittee on Public Buildings and Economic Development. 105th Congress, 2nd Session, 4 June 1998. Washington, DC: U.S. Government Printing Office, 1998. 344p. [Hearing].

SuDoc# Y 4. T 68/2: 105-71

> "Today we are meeting to receive testimony on Federal building security and efforts undertaken by the General Services Administration to enhance a security system in the aftermath of the Oklahoma City bombing in April 1995 … Since then, GSA has taken the lead in national security for Federal buildings."

SECURITY OF U.S. NUCLEAR WEAPONS AND NUCLEAR WEAPONS FACILITIES. U.S. Congress. Senate. Committee on Armed Services. Subcommittee on Strategic. 107th Congress, 1st Session, 13 December 2001. Washington, DC: U.S. Government Printing Office, 2002. 26p. [Hearing].

SuDoc# Y 4. AR 5/3: S.HRG.107-589

> "In this hearing we will cover all aspects of nuclear weapons security, including personnel security, the physical security of sites, security during transportation, emergency response capabilities, and the security features of nuclear weapons themselves."

SECURITY PROCEDURES AT U.S. EMBASSIES. U.S. Congress. House. Committee on Foreign Affairs. Subcommittee on International Operations; Subcommittee on Asian and Pacific Affairs. 96th Congress, 26 February; 26 April 1979; 28 February; 19 June 1980. Washington, DC: U.S. Government Printing Office, 1980. 240p. [Hearing].

SuDoc# Y 4. F 76/1: SE 2/7

> "In a crisis situation Operation Center personnel notify the appropriate action offices in the Department. The Operations Center staff can be immediately augmented if required. And should the situation warrant it, the Executive Secretary can establish a Task Force or Working Group, which brings into special facilities in the Operations Center, personnel from various Department offices and from other agencies as well, to work on the crisis … We feel that this system is more than adequate to provide decision makers with the information that they need to react to any situation … The Department of State communicates with our posts overseas via a number of means depending upon the volume of traffic as well as other factors. This system provides for secure communications, including backup systems that can be utilized if needed."

SECURITY WEAKNESSES AT THE NUCLEAR WEAPONS LABORATORIES. U.S. Congress. Senate. Committee on Governmental Affairs. 100th Congress, 2nd Session, 11 October 1988. Washington, DC: U.S. Government Printing Office, 1989. 478p. [Hearing].

SuDoc# Y 4. G 74/9: S.HRG.100-1053

> "GAO will tell us this morning about instances involving suspected foreign agents of communist nations that have obtained access to our nuclear weapons labs. Of the 181 visitors from communist countries that were surveyed by GAO, DOE failed to obtain necessary background information on 65 percent of those visitors … We will be told that DOE obtained even less information on visitors from other sensitive countries, including several nations suspected of developing nuclear weapons. Of the 637 visitors to these labs from these countries, we will see that DOE only managed to obtain background checks on two percent of these visitors prior to the actual visits. We will hear about a 'Watch List' that was developed by DOE to identify specific foreign organizations suspected of possessing technical capabilities related to nuclear

> weapons. Having developed this list, DOE reportedly did not perform background checks on about 10 percent of the lab visitors who came from these very organizations."

STATUS OF AVIATION SECURITY EFFORTS WITH A FOCUS ON THE NATIONAL SAFE SKIES ALLIANCE AND PASSENGER PROFILING CRITERIA. U.S. Congress. House. Committee on Transportation and Infrastructure. Subcommittee on Aviation. 105th Congress, 2nd Session, 14 May 1998. Washington, DC: U.S. Government Printing Office, 1998. 261p. [Hearing].

SuDoc# Y 4. T 68/2: 105-68

> "Automated passenger profiling is a computer-based method that permits air carriers to focus on the small percentage of passengers who may pose security risks and whose bags should be screened by explosives detection equipment or matched with the boarding passengers. The system developed to screen passengers is known as the computer-assisted passenger screening (CAPS) system. It is designed to enable air carriers to more quickly separate passengers into two categories—those who do not require additional security attention and those who do."

TECHNOLOGY AGAINST TERRORISM: STRUCTURING SECURITY. U.S. Congress. Washington, DC: Office of Technology Assessment, 1992. 142p. [Report].

SuDoc# Y 3.T 22/2: 2 T 27/2

> Interagency coordination of efforts in counterterrorist research and development, integrated security systems, and the role of human factors in aviation security. Details concerning a number of technologies that play a role in counterterrorism.

Online

http://purl.access.gpo.gov/GPO/LPS3622

http://www.wws.princeton.edu/~ota/disk1/1992/9235_n.html

TERRORISM: ARE OUR WATER RESOURCES AND ENVIRONMENT AT RISK? U.S. Congress. House. Committee on Transportation and Infrastructure. Subcommittee on Water Resources and the Environment. 107th Congress, 1st Session, 10 October 2001. Washington, DC: U.S. Government Printing Office, 2001. 147p. [Hearing].

SuDoc# Y 4. T 68/2: 107-51

> "The purpose of this hearing is to make sure governmental agencies and the private sector are taking all the steps necessary to ensure…that the critical infrastructure under our jurisdiction is safe and secure…After September 11, no one who has responsibility for critical infrastructure can ignore the potential for terrorist attacks."

TERRORISM THROUGH THE MAIL: PROTECTING POSTAL WORKERS AND THE PUBLIC. U.S. Congress. Senate. Committee on Governmental Affairs. Subcommittee on International Security, Proliferation and Federal Services. 107th Congress, 1st Session, 30 & 31 October 2001. Washington, DC: U.S. Government Printing Office, 2002. 226p. [Joint Hearing].

SuDoc# Y 4. G 74/9: S.HRG.107-214

> "This new terrorist attack has been difficult to detect and has emerged slowly over a period of weeks … Three people are dead, two of them Postal workers, and at least 10 others have been diagnosed with either cutaneous or inhalation anthrax. Thirty-two people have tested positive for exposure to anthrax and thousands are taking powerful antibiotics as a precaution. In all, Americans are asking themselves a very basic question: Is it safe to open the mail?"

Online

http://purl.access.gpo.gov/GPO/LPS22434

http://purl.access.gpo.gov/GPO/LPS22437 (PDF)

TRANSIT SAFETY IN THE WAKE OF SEPTEMBER 11. U.S. Congress. Senate. Committee on Banking, Housing, and Urban Affairs. Subcommittee on Housing and Transportation. 107th Congress, 1st Session, 4 October 2001. Washington, DC: U.S. Government Printing Office, 2002. 61p. [Hearing].

SuDoc# Y 4. B 22/3: S.HRG.107-620

> "We will be asking all of our witnesses to discuss: First, the existence and nature of any threats to transit. Second, efforts underway to address those threats. Third, lessons learned from the experience of September 11. And fourth, suggestions for improving transit safety."

Online

http://purl.access.gpo.gov/GPO/LPS22816

http://purl.access.gpo.gov/GPO/LPS22817 (PDF)

TRANSPORTATION SECURITY: FEDERAL ACTION NEEDED TO ENHANCE SECURITY EFFORTS: STATEMENT OF PETER GUERRERO, DIRECTOR, PHYSICAL INFRASTRUCTURE ISSUES. U.S. General Accounting Office. 9 September 2003. Washington, DC: U.S. General Accounting Office, 2003. 48p. [Testimony].

SuDoc# GA 1.5/2: GAO-03-1154 T

> "Prior to September 11, the Department of Transportation (DOT) had primary responsibility for the security of the transportation system. In the wake of September 11, Congress created the Transportation Security Administration (TSA) within DOT and gave it primary responsibility for the security of all modes of transportation. TSA was recently transferred to the new Department of Homeland Security (DHS). GAO

was asked to examine the challenges in securing the transportation system and the federal role and actions in transportation security."

Online

http://www.gao.gov/new.items/d031154t.pdf (PDF)

http://www.gao.gov/cgi-bin/getrpt?GAO-03-1154T (PDF)

TRANSPORTATION SECURITY: FEDERAL ACTION NEEDED TO HELP ADDRESS SECURITY CHALLENGES. U.S. General Accounting Office. June 2003. Washington, DC: U.S. General Accounting Office, 2003. 92p. [Report].

SuDoc# GA 1.13: GAO-03-843

"Securing the nation's transportation system is fraught with challenges. The transportation system crisscrosses the nation and extends beyond our borders to move millions of passengers and tons of freight each day. The extensiveness of the system as well as the sheer volume of passengers and freight moved makes it both an attractive target and difficult to secure. Addressing the security concerns of the transportation system is further complicated by the number of transportation stakeholders that are involved in security decisions, including government agencies at the federal, state, and local levels, and thousands of private sector companies … The federal government has provided additional funding for transportation security since September 11, but demand has far outstripped the additional amounts made available. It will take a collective effort of all transportation stakeholders to meet existing and future transportation challenges."

Online

http://purl.access.gpo.gov/GPO/LPS37495 (PDF)

http://www.gao.gov/new.items/d03843.pdf (PDF)

http://www.gao.gov/cgi-bin/getrpt?GAO-03-843 (PDF)

TRANSPORTATION SECURITY: POST-SEPTEMBER 11th INITIATIVES AND LONG-TERM CHALLENGES: STATEMENT OF GERALD L. DILLINGHAM, DIRECTOR, PHYSICAL INFRASTRUCTURE ISSUES. U.S. General Accounting Office. 1 April 2003. Washington, DC: U.S. General Accounting Office, 2003. [Testimony].

SuDoc# GA 1.5/2: GAO-03-616 T

"Since September 2001, securing the nation's transportation systems from terrorist attacks has assumed great urgency. The Congress and the administration have reorganized the federal agencies responsible for transportation security, transferring them to the new Department of Homeland Security, and the agencies are attempting to enhance security without unduly inhibiting the movement of goods and people. The Transportation Security Administration, which was created in November 2001

> and has assumed overall responsibility for transportation security, has made considerable progress in addressing aviation security challenges."

<u>Online</u>

http://www.gao.gov/new.items/d03616t.pdf (PDF)

http://purl.access.gpo.gov/GPO/LPS36497 (PDF)

TRANSPORTATION SECURITY RESEARCH: COORDINATION NEEDED IN SELECTING AND IMPLEMENTING INFRASTRUCTURE VULNERABILITY ASSESSMENTS. U.S. General Accounting Office. May 2003. Washington, DC: U.S. General Accounting Office, 2003. 26p. [Report].

SuDoc# GA 1.13: GAO-03-502

> "The events of September 11, 2001, increased attention on efforts to assess the vulnerabilities of the nation's transportation infrastructure and develop needed improvements in security … The goals of RSPA's Transportation Infrastructure Assurance program are to identify and develop ways to mitigate the impact of, threats to the nation's transportation infrastructure. DOT's Office of Intelligence and Security is responsible for defining the requirements for transportation infrastructure protection, ensuring that vulnerability assessments of transportation infrastructure are conducted, and taking action to mitigate those vulnerabilities."

<u>Online</u>

http://purl.access.gpo.gov/GPO/LPS37003 (PDF)

http://www.gao.gov/new.items/d03502.pdf (PDF)

http://www.gao.gov/cgi-bin/getrpt?GAO-03-502 (PDF)

THE U.S. GENERAL SERVICES ADMINISTRATION'S FEDERAL BUILDING SECURITY PROGRAM. U.S. Congress. House. Committee on Transportation and Infrastructure. Subcommittee on Oversight, Investigations and Emergency Management. 106th Congress, 1st Session, 7 October 1999. Washington, DC: U.S. Government Printing Office, 2000. 74p. [Hearing].

SuDoc# Y 4. T 68/2: 106-46

> "As late as May of 1999 the GSA Inspector General said…the database designed to track information pertaining to security countermeasures installed in Federal buildings nationwide is replete with inaccurate, incomplete, or outdated information, rendering the system useless for ongoing management of security operations or for decision-making purposes…"

U.S. SEAPORT SECURITY. U.S. Congress. Senate. Committee on Commerce, Science, and Transportation. 106th Congress, 2nd Session, 4 October 2000. Washington, DC: U.S. Government Printing Office, 2003. 43p. [Hearing].

SuDoc# Y 4. C 73/7: S.HRG.106-1137

> "Criminal activity at U.S. seaports includes importation of drugs, contraband, and illegal merchandise; stowaways and cargo theft; and the unlawful exportation of controlled commodities, munitions, stolen property, and drug proceeds. Many of these violations are violations of federal law. Additionally, the federal government also has the responsibility of protecting the public from threats of terrorist activity and in ensuring that our transportation strategic needs are not sabotaged."

Online

http://purl.access.gpo.gov/GPO/LPS41687 (PDF)

USDA BIOSECURITY PROGRAMS AND AUTHORITIES. U.S. Congress. House. Committee on Agriculture. 107th Congress, 1st Session, 15 November 2001. Washington, DC: U.S. Government Printing Office, 2001. 39p. [Hearing].

SuDoc# Y 4. AG 8/1: 107-14

> "The attacks of September 11 have led all Americans to reconsider fundamentals. Members of this committee have naturally turned to exploring ways that the food production system can be protected from potential terrorist attacks. We have a responsibility to farmers, ranchers, processors, retailers, and consumers to ensure appropriate steps are being taken to maintain confidence in our food supply."

VULNERABILITY OF TELECOMMUNICATIONS AND ENERGY RESOURCES TO TERRORISM. U.S. Congress. Senate. Committee on Governmental Affairs. 101st Congress, 1st Session, 7 & 8 February 1989. Washington, DC: U.S. Government Printing Office, 1989. 396p. [Hearing].

SuDoc# Y 4. G 74/9: S.HRG.101-73

> "In a world where airplanes with innocent civilians aboard are blasted from the skies in acts of cold-blooded murder, we do not avoid talking publicly about airport security. In like manner, we should examine the robustness and redundancy of our telecommunication and energy networks, and the sufficiency of the government's preparations to assist in reducing existing vulnerabilities gradually over time. In other words, how are we organized, who is responsible, are they on top of what we see as the problem, and are their efforts adequate? … Our country is in a unique situation, because so much of our vital infrastructure is privately owned and operated. These industries are responsive to market conditions. There are some 3,500 electric utilities in this country. Now, how do we deal with all of them and assess the risks posed on each or on the grids into which they feed?"

VULNERABILITY OF THE NATION'S ELECTRIC SYSTEMS TO MULTI-SITE TERRORIST ATTACK. U.S. Congress. Senate. Committee on Governmental Affairs. 101st Congress, 2nd Session, 28 June 1990. Washington, DC: U.S. Government Printing Office, 1990. 151p. [Hearing].

SuDoc# Y 4. G 74/9: S.HRG.101-959

> "Sabotage is particularly worrisome because key facilities can be targeted, and these could take months to repair while large parts of the system are incapacitated. Some of these key facilities are unguarded and in isolated areas. Unless damage is extremely widespread, at least partial power could be restored in a matter of hours. If numerous key pieces of equipment have been destroyed, full restoration might take many months. In the interim, customers would be faced with frequent short-term blackouts and voltage reductions. Economic damage can be very great. Impacts include lost production and sales, damaged equipment and data, public health and safety threats, and the much higher costs of replacement power. An extended power shortage could cost billions of dollars."

WEAK COMPUTER SECURITY IN GOVERNMENT: IS THE PUBLIC AT RISK? U.S. Congress. Senate. Committee on Governmental Affairs. 105th Congress, 2nd Session, 19 May 1998. Washington, DC: U.S. Government Printing Office, 1998. 203p. [Hearing].

SuDoc# Y 4. G 74/9: S.HRG.105-609

> "We must ask whether we are becoming so dependent on communications links and electronic microprocessors that a determined adversary or terrorist could possibly shut down Federal Government operations or damage the economy simply by attacking our computers. At risk are systems that control power distribution and utilities, phones, air traffic, stock exchanges, the Federal Reserve, and taxpayers' credit and medical records."

WEAK LINKS: ASSESSING THE VULNERABILITY OF U.S. PORTS AND WHETHER THE GOVERNMENT IS ADEQUATELY STRUCTURED TO SAFEGUARD THEM. U.S. Congress. Senate. Committee on Governmental Affairs. 107th Congress, 1st Session, 6 December 2001. Washington, DC: U.S. Government Printing Office, 2002. 290p. [Hearing].

SuDoc# Y 4. G 74/9: S.HRG.107-309

> "There are no Federal standards for port security and no single Federal agency overseeing port security. Port security is largely a matter of State and local administration … at any given time, authorities have virtually no idea about the contents of thousands of multi-ton containers traveling on trucks, trains, or barges on roads, rails, and waterways throughout the country. The ease with which a terrorist might smuggle chemical, biological, or even at some point nuclear weapons into one of those containers without being detected is terrifying."

Online

http://purl.access.gpo.gov/GPO/LPS22199

http://purl.access.gpo.gov/GPO/LPS22200 (PDF)

WEAK LINKS: HOW SHOULD THE FEDERAL GOVERNMENT MANAGE AIRLINE PASSENGER AND BAGGAGE SCREENING? U.S. Congress. Senate. Committee on Governmental Affairs. Subcommittee on Oversight of Government Management, Restructuring, and the District of Columbia. 107th Congress, 1st Session, 25 September 2001. Washington, DC: U.S. Government Printing Office, 2002. 165p. [Hearing].

SuDoc# Y 4. G 74/9: S.HRG.107-208

> "The General Accounting Office has determined that undercover agents have been able to penetrate restricted areas of U.S. commercial airports with counterfeit or otherwise invalid badges or other credentials, giving those agents the opportunity, if intended, to carry weapons, explosives, other things that are dangerous to the security of everyone."

Online

http://purl.access.gpo.gov/GPO/LPS21053

http://purl.access.gpo.gov/GPO/LPS21054 (PDF)

WHAT CAN BE DONE TO REDUCE THE THREATS POSED BY COMPUTER VIRUSES AND WORMS TO THE WORKINGS OF GOVERNMENT? U.S. Congress. House. Committee on Government Reform. Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. 107th Congress, 1st Session, 29 August 2001. Washington, DC: U.S. Government Printing Office, 2002. 184p. [Hearing].

SuDoc# Y 4. G 74/7: V 81/4

> "So far, these viruses and worms have not caused irreparable damage to the Federal Government's information systems. However, as the attacks become more sophisticated, the magnitude of the potential threat is colossal. We must do something more than just react to these attacks. There is no easy fix but governments at every level must be prepared for the next attempted invasion. Computer security must have a priority. Today we will examine the extent of the threat to government computer systems and the need for policy changes to ensure that these systems which are vital to this Nation and its economy and its citizens are protected."

Online

http://purl.access.gpo.gov/GPO/LPS22295

http://purl.access.gpo.gov/GPO/LPS22296 (PDF)

WHAT REGULATIONS ARE NEEDED TO ENSURE AIR SECURITY? U.S. Congress. House. Committee on Government Reform. Subcommittee on Energy Policy, Natural Resources, and Regulatory Affairs. 107th Congress, 1st Session, 27 November 2001. Washington, DC: U.S. Government Printing Office, 2002. 126p. [Hearing].

SuDoc# Y 4. G 74/7: R 26/20

> "The tragic events of September 11, 2001, have shaken the confidence of the U.S. Government and its citizens in the Nation's air security. Immediately after September 11th, the President and Congress began to examine the existing system, including the laws, regulations and actual practices governing air security. Much was found to be lacking. Some changes were made immediately by the President, such as having more law enforcement officials on airplanes and in airports. Other changes were quickly made by the airlines, such as locking all cockpit doors. On November 19th, the President signed a comprehensive Aviation and Transportation Security Act written by this Congress. This law places responsibility for air security in the hands of the Department of Transportation. Within 1 year, DOT is required to primarily use Federal employees for passenger and baggage screening …Today, we plan to examine how to make this new system work."

Online

http://purl.access.gpo.gov/GPO/LPS26862 (PDF)

WHAT REGULATIONS ARE NEEDED TO ENSURE PORT SECURITY? U.S. Congress. House. Committee on Government Reform. Subcommittee on Energy Policy, Natural Resources and Regulatory Affairs. 108th Congress, 1st Session, 24 April 2003. Washington, DC: U.S. Government Printing Office, 2003. 179p. [Hearing].

SuDoc# Y 4. G 74/7: R 26/21

> "The Maritime Transportation Security Act raises questions about the right balance between increasing port security on the one hand and not impeding the flow of commerce and trade on the other. Standard versus port-specific security measures— in other words, what is our national standard and what are the unique circumstances of any given port? And also, what is the role of government in solving these problems, as opposed to the role of private industry?"

Online

http://purl.access.gpo.gov/GPO/LPS35558 (PDF)