# Grants Funding

Grade: D+

*In FY2007, the Administration again failed to fund the Urban Area Security Initiative at adequate levels. New York City is still only receiving 18% of the total pot, compared to the 25% it received in 2005*.

- **Despite the 9/11 Commission's recommendation that funds be distributed based on threat and risk assessments, DHS continues to dictate that funding be allocated by the old formula in the USA Patriot Act**. This formula unfairly guarantees each state a minimum of 0.75% of total appropriations for domestic preparedness programs. This problem will be somewhat remedied in the next fiscal year with the enactment of the 9/11 Commission Recommendations Act, (P.L. 110-53) which will lower the minimum allocation for each state to 0.375% of total SHSGP and UASI appropriations in FY2008, with the floor eventually reduced to 0.35% of the total SHSGP and UASI appropriations in FY2012.

- **DHS continues to use an outdated and convoluted threat and asset database to calculate how much money high threat areas receive.** Last year, according to a new audit from the Department of Homeland Security Inspector General's office, dozens of questionable locations around the country are counted as terrorist targets, including a petting zoo in Woodville, Alabama, a "Mule Day" Parade in Columbia, Tennessee, and the Amish Country Popcorn Company, which has five employees in Berne, Indiana who grow and distribute popcorn. In the report, Indiana had 50% more terrorist targets listed than New York (5,687) and twice as many as California (3,212). The DHS inspector general found that the Department relied on this dysfunctional database when making critical funding decisions.

**Improvements Expected in the Next Year:**

  - **The new Congress has taken steps to restore funding cuts made by the administration to state and local programs in the Department of Homeland Security.** In July, the Senate approved an FY2008 DHS appropriation of $4,136 million for state and local programs, which is $749 million more than the FY2007 total appropriation of $3,387 million.

  - **For the upcoming year, the Senate recommended increasing the overall UASI appropriation for FY2008 to $820 million, just below the FY2005 amount of $833 million.** This is a great improvement over the last two years, demonstrating again the Democrats' commitment to homeland security.

Grade: F

# Preparedness & Response

- **While communications problems were the main obstacle for first responders in the wake of 9/11, the current Administration failed in the six years following the attacks to properly fund the creation and implementation of an interoperable communications system in New York or anywhere else throughout the country.** In fact, according to a scorecard released by the Department of Homeland Security in January, only six of seventy-five urban and metropolitan areas graded for their interoperable communications systems received top marks. New York ranked fourteenth on the list.

*(continued from page 1)*

- **DHS still has no requirement for states to produce a comprehensive plan for an interoperable communications system to receive communications grants and no national plan to coordinate investments across states.** For example, while New York is currently in the process of deploying the Statewide Wireless Network for $2 billion, localities are not required to participate, and local interest in the statewide system has been limited. As a result, localities are continuing to develop their own interoperability solutions that do not incorporate the network. Because of the lack of coordination, state and local governments are investing significant resources, including DHS grant funds, in developing independent interoperability solutions that do not always support each others' needs.

- **DHS has failed to meet five major goals related to helping improve interoperability.** According to a comprehensive GAO report released this week, DHS has not met five specific performance goals related to interoperability including increasing the development and adoption of interoperability communications standards and providing guidance and technical assistance to first responders in developing and implementing interoperable communications capabilities.

- **According to a January report by the Government Accountability Office, the Department of Defense has no adequate measures in place to determine the readiness of National Guard forces for an attack or natural disaster.** Since the start of the war in Iraq, the National Guard has seen its largest overseas deployment since World War II, leaving staffing and equipment levels at home strained and possibly insufficient in the event of another attack. The Chief of the National Guard Bureau has reported that his forces have less than 34% of the equipment they should have in the event of an attack.

- **First Responders still lack the life-saving equipment they need to do their jobs safely and effectively.** On September 11, 2001, first responders rushed to the scene and risked their lives to help those affected, but six years after the attacks the federal government has failed to equip them with the necessary tools to respond should there be another attack. This year alone, New York police officers responded to the Midtown steam pipe explosion without gas masks to protect themselves from the asbestos that spewed into the air, and the New York Police Department was forced to recall 20,000 gas masks that the manufacturer deemed defective.

# Aviation Security

Grade: C+

*In the immediate aftermath of the September 11, 2001 terrorist attacks, Congress acted quickly to address the gaping holes in our aviation security system and passed the Aviation and Transportation Security Act, which created the Transportation Security Administration (TSA) and a federalized force of security screeners to inspect passengers and luggage. Post-9/11 security upgrades also included in-flight measures, such as the expansion of the Federal Air Marshal Service (FAMS) and the installation of hardened cockpit doors.*

- **Just this past week, a Justice Department audit discovered that the FBI failed to put as many as 20 names of suspected terrorists on the watch lists it maintains.** Over the last two years, the FBI has tried to consolidate the more than 700,000 records it maintains on suspected terrorists. The 9/11 Commission called for a single agency to consolidate and manage the 12 separate watch lists that were in use prior to the September 11th terrorist attacks. However, problems have persisted in the technology used, and the names of 20 suspected terrorists were not listed.

- **A July 2007 internal audit by the Inspector General of DHS blasted TSA's ability to screen the 7,500 tons of air cargo carried aboard passenger aircraft each day.** Experts believe that cargo is serious target for terrorists, yet according to the audit, only a small fraction of that cargo is actually screened. It also reveals that TSA lacks a "comprehensive, consistent and reliable program" to screen passenger air cargo, nor does the current regime ensure that carriers are screening in a manner consistent with federal regulations.

- **TSA has only 300 cargo-specialists to conduct inspections of screening practices at 100 airports.**

*(continued from page 2)*

- **In March, airport employees at Orlando International Airport were arrested for smuggling guns aboard a commercial airliner, a glaring example of the need for screening of airport employees.**

- **DHS still has not deployed a comprehensive system to check if a terrorist has bought an airline ticket.** While over $170 million has been spent on the Secure Flight program—a system that would match airline passengers against terrorist watch lists—the Government Accountability Office (GAO) reports that it faces considerable management and oversight challenges. The program has already been suspended only to later be resumed. This is the third time since 9/11 that DHS has attempted to implement a plan to check passenger names against a terrorist watch list. Secure Flight is the successor to the controversial and never-deployed CAPPS II, which was widely criticized by privacy advocates and Congress for being too intrusive in to the passenger data it planned to collect.

- **Technology to screen passengers for weapons and explosives is years behind where it needs to be.** According to Congressional Research Service, only 114 detection portals, or "puffers," have been deployed in 30 airports since 2004 and none have been deployed since 2006. (The portal systems cost approximately $160,000 each.) There are still many outstanding reliability and maintenance issues associated with the puffer technology, particularly a high rate of false alarms and tendency to break down after a short period of usage. In fiscal year 2007, Congress gave TSA $4.73 billion specifically designated for aviation security. But out of that total, only $501 million–about 10%–went to explosive detection on passengers and carry-on bags.

- **TSA has done very little to ensure that foreign airports are complying with international security standards, and has made a mediocre effort to coordinate with foreign governments. Currently, TSA only has 21 inspectors stationed abroad in 14 countries as security coordinators and points-of-contact for foreign government officials.** These Transportation Security Administration Representatives (TSARs) are stationed around the world to "promote alignment and consistency, conduct airport assessments, consult with the host country on aviation security matters, serve as on-site coordinators for TSA in the event of a terrorist attack, and ensure air carriers are complying with U.S. regulations." Although there are an additional 75 International Aviation Inspectors, there are not nearly enough TSARs deployed worldwide to make certain that foreign airports are in compliance and operating at an appropriate level of security.

- **There is no standard, tamper-proof, biometric identification card for airport workers which would prevent a terrorist from sneaking onboard a flight without a boarding pass, or breaking into secure areas.** Last year, TSA began to roll out its plan for a biometric identification card for seaport workers, but there is no plan to extend the Transportation Worker Identification Credential (TWIC) program to the aviation sector any time soon. TWIC is a tamper-resistant credential that contains biometric information about the holder which renders the card useless to anyone other than the rightful owner. TWIC can verify the identity of a worker and help prevent unauthorized individuals from accessing secure areas. Airports can employ thousands of people, and it is essential that there be a standard, tamper-proof identification card to keep terrorists out of sensitive and secure airports. The program was originally scheduled to be deployed years ago at ports, airports, and transportation facilities across the country, but it had been repeatedly delayed due to political wrangling and mismanagement by DHS.

- **DHS has not addressed its primary goals when it comes to protecting secure areas of airports and air cargo.** According to the GAO, in addition to failing to implement systems to adequately screen air cargo, DHS has also failed to establish standards to secure airport perimeters and background checks for airport workers.

**<u>Improvements Expected in the Next Year:</u>**

- **The new Congress has made huge strides to enhance aviation security through numerous measures included in the 9/11 Commission Recommendations Act of 2007.** Until now the Administration had placed a cap of 45,000 on the number of TSA screeners at the roughly 500 commercial airports nationwide. The imposition of this cap forced TSA to cut the number of screeners from a previous high of 51,000-52,000 just after 9/11. Under the new law, TSA is directed to hire as many screeners as necessary to ensure adequate aviation security and reduce average security-related delays to less than 10 minutes.

*(continued from page 3)*

- **To address the gaping hole in air cargo screening on passenger flights, this legislation requires the TSA to establish a system for screening 100% of cargo within three years, with an interim requirement of screening 50% of such cargo within 18 months of enactment.** Congress will be watching TSA and the airline industry very closely to ensure that neither party attempts to circumvent the 100% screening requirement by allowing sealed boxes sent by approved shippers to be loaded on to passenger planes, thus reviving parts of the known shipper program.

Grade: B-

# Nuclear, Chemical & Biological Security

**Nuclear Security—***Terrorists could cause untold loss of life, health risks, and economic damage by detonating a nuclear weapon or a "dirty bomb" that uses a conventional explosive to disperse radioactive material. It is essential that the United States guard against these threats by securing existing radioactive sources and sites and by deploying accurate detectors at ports of entry and within the country.*

- **Covert investigations by the GAO have repeatedly found dangerous weaknesses in how the Nuclear Regulatory Commission (NRC) licenses companies to purchase nuclear materials.** NRC is charged with regulating sealed radioactive sources inside the United States. One recent GAO report revealed that investigators used publicly available information to obtain a license for radioactive materials in the name of a company created to be a false front for this purpose. Clearly, the NRC has failed to assess and address persistent loopholes in licensing security despite following up on earlier probes, including a 2006 report documenting GAO investigators' ability to bring radioactive materials across U.S. land borders with counterfeit licenses.

- **There are still gaping holes in security at nuclear power plants in New York and across the country. In August 2007, an armed guard in an inner security ring around the Indian Point nuclear plant, 35 miles north of Manhattan, was found asleep by an NRC inspector and took nearly two minutes to awaken.** Although no known security breach occurred, this incident is chilling proof of vulnerabilities in nuclear plant security. On April 18, 2007, a final NRC rule went into effect to update nuclear plant security. Though the rule is classified, the NRC has been criticized because the new rule does not require plants to defend against an aircraft attack.

- **Current disaster planning still may not accurately reflect the risks of nuclear attack.** Every nuclear plant is surrounded by an Emergency Planning Zone, within which plants must install sirens and conduct evacuation drills, and residents can get supplies of iodine pills to prevent radiation contamination. The NRC has set this zone at approximately ten miles. Since 9/11, there have been calls to extend the Emergency Planning Zone to a larger distance such as 50 miles, to better reflect the reach of a nuclear incident. With a 50-mile perimeter, Manhattan would be included in emergency planning for any disaster at the Indian Point nuclear power plant.

- **DHS is still struggling to purchase radiation detection equipment that meets security needs.** Serious questions have been raised about the government's procurement of the next generation of radiation detection portal monitors, known as Advanced Spectroscopic Portals (ASPs). The GAO has reported that the decision to purchase and deploy new ASPs, which cost six times more than current technology, is not supported by the cost-benefit analysis performed by the Domestic Nuclear Detection Office (DNDO).

**Chemical Plant Security—***Although in the past year we have seen strides toward a more secure chemical infrastructure, exploiting its remaining weaknesses will no doubt remain attractive to terrorists. With some 15,000 hazardous facilities in the United States—over a hundred of which, if attacked, would threaten more than one million people—chemical plants are potentially catastrophic soft-targets.*

- **DHS still only has a patchwork of federal regulations to beef up security at chemical plants.** The Department of Homeland Security recently released its interim final rule regarding the security of chemical facilities. The regulations require chemical facilities in possession of certain amounts and types of substances considered hazardous by the DHS Secretary to notify DHS. **However, only if chemical facilities are deemed "high-risk" by the DHS Secretary are they required to meet security standards.** This potentially leaves exposed thousands of lesser-risk, but still dangerous, facilities.

- **Comprehensive regulations still do not exist concerning the security of drinking water and wastewater treatment facilities that house the hazardous chemicals (such as chlorine gas).** Moreover, security of these facilities has been deemed a responsibility of the Environmental Protection Agency by the President. The DHS and the EPA have yet to enter into the comprehensive memorandum of understanding defining the relationship and responsibilities of the two agencies with regard to securing critical infrastructure directed by an act of Congress in 2005.

**Improvements Expected in the Next Year:**

  - **The Senate-passed version of the Department of Homeland Security Appropriations Bill for FY2008 contains a provision to regulate the sale and transfer of ammonium nitrate – a popular fertilizer that is also a common ingredient of truck bombs.** The bomb that exploded in Oklahoma City in 1995 was made of ammonium nitrate, mixed with fuel oil to render it combustible. It is shocking that in twelve years since that tragedy, the federal government has done little to prevent the use of ammonium nitrate in terror attacks.

**Biosecurity—***The Administration has yet to devise a coherent, comprehensive and strategic biodefense plan. Because there are a myriad of agents that could potentially be used as bioweapons, it is imperative that the issue be addressed. In addition to casualties, a biological attack could have catastrophic effects on our agriculture and economy, and our public health systems are currently unprepared to cope with such an event.*

- **The Administration has failed at effectively implementing its primary program to protect millions from a biological attack, but Congress has taken positive steps to fix the program.** Three years after Congress created "Project Bioshield", which was supposed to be an elaborate national stockpile of drugs and other measures to counter the effects of biological and radiological weapons, the Administration still has not implemented it fully as it has been plagued by delays and bureaucratic fumbles. In an attempt to repair the program, Congress created the Biomedical Advanced Research and Development Authority (BARDA), an office within the Department of Health and Human Services, in the Pandemic and All-Hazards Preparedness Act. BARDA's mission is to improve "Project Bioshield" by supporting, coordinating, and providing oversight of advanced development of vaccines and biodefense countermeasures.

**Improvements Expected in the Next Year:**

  - **The new Congress has taken steps to improve coordination on biosecurity matters.** The 9/11 Commission Recommendations Act of 2007, which was signed into law last month, authorizes the National Biosurveillance Integration Center. The Center is tasked with identifying and monitoring important biological events by integrating and analyzing data from human health, animal, plant, food, and environmental monitoring (surveillance) systems; and communicating information to other federal agencies and to state, local, and tribal governments, to enhance national response capability.

# Mass Transit & Truck Security

Grade: D+

*Mass transit systems have been a prime target for terrorists for decades. Despite the obvious threat, prior to 9/11 many stations were not equipped with closed-circuit security camera systems and bomb detectors were only deployed in extraordinary circumstances. In the wake of the 9/11 attacks, local and federal law enforcement stepped up police presence at stations and deployed bomb-sniffing dog teams, but there was no advanced technology available to immediately detect the presence of a nuclear, biological, chemical, or explosive device. DHS has only issued voluntary security guidelines for transit operators.*

- **Six years after 9/11, research and development into new explosive, radiological, chemical, and biological detectors is still in the early developmental stages.** TSA created a mass transit security pilot program in 2004 called the Transit and Rail Inspection Pilot (TRIP), however this pilot was completed in 2006 and has yet to be permanently implemented anywhere in the country. In addition, even after train bombings in Madrid, London, and Mumbai, TSA did not mandate that rail or mass transit systems install technology that could detect explosive devices.

- **TSA does not currently have the personnel to adequately ensure the security of our nation's rail and mass transit systems.** In contrast to the roughly 44,700 aviation screeners, there are only 100 surface inspectors. These inspectors are charged with covering more than 300,000 miles of freight rail lines, which are also used by Amtrak passenger trains, and 10,000 miles of commuter and subway rail lines. To make matters worse, according to testimony from the Federal Railroad Administration (FRA) included in a GAO report, less than a quarter of the nation's 400,000 transit employees have received security training.

- **Six years after 9/11, DHS still has not issued mandatory security requirements to protect transit systems.** In May 2004, DHS issued a number of voluntary directives which called on major transit operators to enhance physical security by, among other measures, installing transparent bomb-resistant trash cans, deploying additional police and security personnel, installing closed-circuit security cameras, and conducting random inspections of passengers and bags. DHS has done little to ensure that these directives have been followed even after the bombings in Madrid, London, and Mumbai. In fact, a recent GAO report acknowledged some of these directives "may not provide the industry with baseline security standards based on industry best practices." Furthermore, some of these DHS directives are in direct conflict with previous FRA safety regulations. For example, FRA requires that engineer compartment doors be unlocked to aid emergency escapes while DHS requires that doors equipped with locks remain locked. Conflicting safety measures highlight the inadequacy and inefficiency of security requirements for the transit system.

- **Even though two of the last three major mass transit attacks occurred on above ground, longer distance commuter lines, Amtrak and regional commuter rail systems remain woefully unprotected.** According to a March 2006 report by the Government Accountability Office, since the September 11 attacks, basic security features such as more security personnel and control of access to train stations, have not been put in place by all commuter rail systems. In addition, the Hudson River tunnels used daily by Amtrak are nearly 100 years old and not likely to withstand an attack. TSA has testified that underground tunnels are one of the highest security priorities within the mode-specific plans developed by DHS this year.

- **DHS and TSA continue to spend, on average, $9 per air passenger, as compared to only one penny per rail/mass transit rider.** According to the American Public Transportation Association, it will take more than $6 billion to secure mass transit stations across the country.

- **Three years after DHS was directed to prepare a national strategy for transportation security, mode-specific security plans have not yet been completed.** The Intelligence Reform and Terrorism Prevention Act of 2004 directed DHS to create a national strategy for transportation security. This plan would identify national transportation assets, set risk based priorities for their protection, assign responsibilities for their protection, and recommend appropriate levels and sources of funding for these efforts. DHS finally announced the plan's release in May 2007. However, GAO has merely called this a first step. Although the plan describes how the most critical transportation assets will be identified and how their risk will be assessed, it still does not include how risks to transportation assets are actually being assessed and protected.

*(continued from page 6)*

**Improvements Expected in the Next Year:**

- **The new Congress has attempted to address the nation's mass transit security needs by increasing funding for grants that can be used to improve safety and by imposing more security requirements on rail operators.** The 9/11 Commission Recommendations Act of 2007 includes:
  - $3.4 billion for grants for public transportation security of which $840 million can be used for security-related operating expenses and an additional $100 million for research and development; $1.2 billion for grants for railroad security; an additional $650 million for Amtrak security upgrades; an additional $200 million is for safety improvements to rail tunnels in NY, Baltimore and DC; and $95 million for grants for over the road bus security
  - Authorization to hire and funding for up to 100 more surface transportation security inspectors
  - Requirement that DHS conduct a name-based security background check and an immigration status check on all public transportation and railroad frontline employees
  - Authorization for DHS to regulate security training the training of rail employees

*Terrorists have used trucks to attack Americans around the world and on our own soil – in New York City at the World Trade Center in 1993, in Oklahoma City, and at our military compound in Dhahran, Saudi Arabia. Prior to 9/11, the government did very little to track shipments of hazardous materials or perform background checks for any of the drivers who haul these materials.*

- **The Administration has failed to adequately protect communities from the threat posed by trucks carrying dangerous chemicals, but Congress has recently taken steps to address this security problem.** Despite the fact that numerous trucks cross the country daily carrying potentially deadly chemicals like ammonium nitrate, chlorine, and cyanide, DHS still has not come up with a comprehensive system to track these hazardous materials. According to the 1997 Census of Interstate Commerce, 740,000 hazardous materials shipments travel by truck each day in the United States. Approximately 50,000 trips are made daily by gasoline tankers, many of which hold as much fuel as a Boeing 757. Although many of our nation's larger trucking companies have voluntarily placed GPS tracking devices on their trucks, there is still no federal center to track truck shipments across the country.

- **DHS still has not completed full background checks of truck drivers licensed to carry hazardous materials.** DHS initiated a program in 2003 to run background checks on drivers licensed to carry hazardous materials, but this process is not expected to be completed until 2010. The program has been plagued by administrative delays and bureaucratic tangles between state and federal transportation officials.

**Improvements Expected in the Next Year:**

- **The new Congress passed the Schumer Amendment that requires TSA to establish and implement a program to track trucks carrying hazardous material.** Trucks carrying high hazard materials (materials that are toxic, radioactive, etc.) pose a threat to our national security if they fall into the hands of terrorists. Schumer's amendment to the 9/11 Commission Recommendations Act of 2007, which became law in August, requires the DOT and the TSA to develop a system to track freight trucks carrying high hazardous materials. In addition, DOT and TSA would evaluate technology that includes the installation of devices on these trucks to safely disable the vehicle if it strays from a predetermined route, and report back to the Congress in one year.

Grade: C-

# Port Security

*Currently, cargo containers routinely travel the seas with minimal tools to detect or prevent tampering–merely a flimsy plastic or wire loop placed around the container doors and marked with a unique number. These lightweight "seals" may provide warning of tampering, but don't prevent intrusion. The SAFE Port Act of 2006 required DHS to establish requirements for securing cargo containers in transit by April 2007, but DHS missed this deadline and still has not issued requirements.*

- **The DHS Appropriations bill passed by the Senate in August 2007 would provide $400 million for port security grants across the country**. So far in 2007, entities affiliated with the Port of New York and New Jersey have been awarded a total of approximately $19.7 million in federal grants to improve port security. In May, the Port of Albany and Rensselaer was awarded $351,000, and the Port of Buffalo was awarded $220,456. Unfortunately, this bill faces a likely veto threat because the Senate and House have sought to fund priorities in amounts that exceed the President's insufficient budget request.
- **TSA has now missed two deadlines to implement TWIC cards at seaports across the country.** TSA is required by law to develop biometric credentials for access to secured areas in seaports and is using the maritime environment to launch new Transportation Worker Identity Credential (TWIC) cards, which will eventually be used across all transportation modes for workers who require unescorted access to secure areas. TSA failed to meet a July 1, 2007 deadline for implementing the TWIC program at the ten highest-risk U.S. ports, after missing an April deadline to begin pilot testing technology to read TWIC cards at five ports by April 2007.

- **The U.S. Coast Guard missed the April 1, 2007 deadline to implement a long-range tracking system for vessels approaching U.S. ports.** Not until the end of 2007 does the Coast Guard anticipate providing continuous satellite tracking of vessels headed for the Port of New York and New Jersey.

- **Despite new legislation passed this year, the President did not request funding for cargo scanning priorities in FY2008.** In contrast, both the Senate and House appropriations bills proposed increases in funding for port security priorities like additional Customs and Border Patrol (CBP) inspectors, Coast Guard operations and maritime operational centers, and developing new and better detection capabilities.

- **The SAFE Port Act required DHS to establish a pilot project in three ports overseas to scan cargo containers for radiation before they reach the shores of the United States.** The pilot project is due to be fully implemented by October 13, 2007. So far, DHS has fully implemented the project at only two ports overseas, in Honduras and Pakistan. DHS estimates that they will meet the mid-October deadline for establishing the pilot project at the third port, in the United Kingdom. Each of these three ports will scan 100% of their U.S.-bound cargo. DHS also plans to implement some cargo scanning at an additional four overseas ports, expanding on the mandate in the SAFE Port Act. Taken together, these overseas ports will scan approximately 8% of the maritime containerized cargo that arrives at U.S. shores each year.

*(continued from page 8)*

**Improvements Expected in the Next Year:**

- **The 9/11 Commission Recommendations Act of 2007, signed by the President on August 3, provides the strongest mandate yet to scan incoming cargo containers for nuclear and radiological devices.** Under this new law, within five years, 100% of containers must be scanned before they leave foreign ports bound for the United States. However, the law contains a potential loophole: the Secretary of Homeland Security may extend this deadline by two years if certain conditions are met, and the extension is renewable in two-year increments.

- **Congress advanced port security significantly in the past year with the passage of the Security and Accountability for Every Port Act of 2006 (the SAFE Port Act).** Among other provisions, this Act codified two major maritime security programs: the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT). The law established the Domestic Nuclear Detection Office (DNDO) within DHS, included mandates for implementing the Transportation Worker Identification Credential (TWIC) program, and boosted programs for developing new devices to detect threats in ports. It also required the installation of radiation detection equipment at all U.S. ports by the end of 2006, and it established a pilot program at a few foreign ports to scan all cargo containers bound for the United States.

- **Under the SAFE Port Act, all cargo containers entering the United States from overseas must be screened to identify high-risk containers.** Cargo containers identified as high-risk must be scanned for radiation or searched before leaving the seaport. As of August 31, 2007, DNDO reports that it has installed 1,019 radiation portal monitors at 86 ports of entry, resulting in 92% of the incoming container cargo being screened before it leaves the seaport of arrival.

# Border Security

Grade: C

- **As of late last year, our Northern Border was still short—by more than 1,000 border agents—of the 5,000 required by law.**

- **On May 24, 2007, a traveler infected with a dangerous form of tuberculosis entered the United States despite official warnings that he should be stopped at the border.** The widely-publicized incident raised serious and pressing questions about CBP staffing and training at land ports of entry, as well as U.S. preparedness to confront public health threats. In 2006, covert GAO investigators were able to enter the United States from Canada and Mexico using fake driver's licenses and other documents. The GAO found that "this vulnerability potentially allows terrorists or others involved in criminal activity to pass freely into the United States from Canada or Mexico with little or no chance of being detected."

- **The State Department significantly underestimated the increase in passport demand that coincided with the new rules requiring passports or other secure citizenship documentation for visitors and citizens arriving in the United States by air.** Enormous backlogs in processing forced DHS to suspend the new documentary rule from early June until September 30, 2008. With the goal of ensuring a smooth transition to any further border rules, both the House and the Senate have now voted to provide that passport rules may not be implemented at land and sea ports of entry prior to June 1, 2009.

*(continued from page 9)*

- **The security of government travel documents, which provide a literal key to the country, remains a major issue.** The State Department (working with DHS) plans to offer new People Access Security Service (PASS) cards containing radio frequency identification technology for crossing Western Hemisphere land borders. But in May 2007, representatives of the State Department and DHS admitted to Senator Schumer that they had not yet conducted any field testing of the proposed card architecture to assure security, efficiency and reliability. To this day, they have yet to do so. Any international travel document issued by the United States must be completely secure. Until DHS issues a final regulation, far too many questions regarding the proposed PASS cards will remain unanswered.

- **DHS is struggling to develop a required biometric system for tracking the arrivals and departures of foreign visitors to the United States, a program known as U.S. Visitor Immigrant Status Indicator Technology (US-VISIT).** DHS has implemented the entry portion of US-VISIT at nearly 300 airports, seaports, and land ports of entry. However, DHS admits that US-VISIT has no ability to track exiting travelers despite spending $250 million on this effort over the past four years. Moreover, DHS has no near-term solution for biometric tracking of land exits, a hole that renders the entire system virtually ineffective. In July 2007, the GAO found "significant weaknesses" in the information systems that support US-VISIT and other CBP programs, creating vulnerabilities that attackers could use to disrupt operations or change records. The GAO also found in July that the US-VISIT program suffers from a "long-standing lack of strategic direction and management controls" and concluded that DHS's new effort to establish an exit tracking capability is not likely to succeed without significant reforms.

**Improvements Expected in the Next Year:**

- **The FY 2008 DHS Appropriations bill, passed by the Senate in early August, provides funds to hire 3,000 new Border Patrol agents and support staff and $1 billion for border fencing, infrastructure, and technology.**