# ASIS International Federal and Legislative Policy Update

September 2011

## Anti-Piracy

ASIS recently has been in discussions with the Motion Picture Association of America (MPAA) regarding S.968, the "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011," or the "PROTECT IP Act of 2011."

This important legislation was introduced in the Senate Committee on the Judiciary in May, 2011. We recently became involved because the bill was reported out of the Senate Judiciary Committee just before August recess. It may move quickly. It was sponsored by Judiciary Committee Chairman Patrick Leahy (D-VT) and has 29 co-sponsors. They include 16 Democrats, 12 Republicans and one Independent from all parts of the political spectrum.

The bill is a potentially powerful vehicle to shut down foreign websites dedicated to the unauthorized distribution of licensed content and counterfeit goods. It is focused on sites registered outside the U.S., where some of the most brazen offenders operate outside the jurisdiction of U.S. prosecutors and legal authority. Protect IP would allow the U.S. Department of Justice (DOJ) or copyright holders themselves to seek court orders restraining access to rogue sites, effectively shutting them down. The DOJ's enforcement authority would augment the "notice and takedown" provisions of the 1998 Digital Millennium Copyright Act, which allows copyright and trademark holders to quickly remove infringing content from websites registered within the U.S.

S. 968 would prevent Internet service providers and search engines from directing traffic (including hyperlinks) to offending sites. It also "Directs the (U.S. Attorney General) AG to identify and provide advance notice to…financial transaction providers (FTPs), Internet advertising services (IASs), and providers of information location tools (ILTs)…whose action may be required to prevent such… activity." In other words, it encourages those who might advertise on such sites and those who process their financial transactions to desist and it offers legal immunity to those who voluntarily cease operations with sites believed to be "dedicated to infringing activities." We believe this is the bill's major strength. If advertisers will not buy space on these sites, and financial transaction providers will not process their transactions, they will be seriously reduced in their capacities.

The list of counterfeit goods that are pushed through these sites is huge, from pharmaceuticals to movies to safety and security equipment. The list of supporters of this bill is likewise huge. It includes the US Chamber of Commerce, pharmaceutical manufacturers, owners of intellectual property (including major studios and publishers), the national sports leagues, major retail chains, clothiers, and manufacturers of all types.

There is opposition, as well. Several credit card companies are opposed, likely because of concerns over the complexity, cost and liability (though the law indemnifies them) that might be involved in refusing to conduct transactions. Google and several foundations and associations

are opposed due to their concerns that the legislation abridges freedom of expression via the Internet. It hardly seems realistic, however, that liberal Democratic Senators would support, let alone sponsor, such a bill.

ASIS is submitting letters of support for S. 968 to key offices in the House and Senate.

## Chemical Security

As the latest extension of DHS's authority to set performance standards at high-risk chemical facilities, known as CFATS (Chemical Facility Anti-Terrorism Standards), is set to expire in October, Congress is considering a number of bills that would extend the program for several years.

H.R. 908, introduced by Rep. Tim Murphy (R, PA-18th), provides a 7-year clean extension of CFATS (no IST language) and would authorize nearly $90 million annually for the program. This bill passed the House Energy & Commerce Committee on May 26th and awaits action on the House floor.

H.R. 901, introduced by Rep. Dan Lungren (R, CA-3rd), also provides a 7-year extension and $93 million annually, but would do so by adding CFATS authorization to the law that created the Department of Homeland Security. This would consolidate jurisdiction over chemical facilities within the Homeland Security Committee, rather than Appropriations. This bill passed the House Homeland Security Committee in June, but is also referred to the House Energy & Commerce Committee, where it awaits action.

S. 473, introduced by Sen. Susan Collins (R-ME), provides a 3-year extension and includes voluntary training and technical assistance programs. This bill was reported out of the Senate Homeland Security and Governmental Affairs Committee in June, but has not come up for a floor vote in the Senate.

Note: Language in the Homeland Security Appropriations bill, H.R. 2017, which passed the House and is awaiting a vote in the Senate, would reauthorize CFATS through Oct. 4, 2012. It is expected that separate CFATS legislation also will be passed during the 112th Congress.

## Cybersecurity

### House Proposals:

A series of new cybersecurity proposals have been under discussion in the House since Congress returned from August recess.

Rep. Dan Lungren (R, CA-3rd), Chair of the House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, has circulated a draft bill that aims to clarify DHS's authority to manage the security of federal cyber and critical infrastructure systems. According to the draft, the bill would create a National Information

Security Organization (NISO), a non-profit organization tasked with sharing cyber threat information and developing information security technology. The NISO would act as a clearinghouse for the exchange of cyber threat information between the federal government, critical infrastructure owners and operators, state and local governments and the private sector.

Another provision would establish the U.S. Computer Emergency Response Team within DHS that would be responsible for coordinating a response to cyber incidents, facilitating information sharing between the public and private sector and disseminating information about cyber threats.

Sec. 227 of the draft would establish voluntary, risk-based performance standards and practices for private sector information security systems, and would ensure that they are evaluated and updated annually.

Rep. Bob Goodlatte (R-VA, 6th), Chair of the House Judiciary Subcommittee on Intellectual Property, Competition and the Internet, is considering drafting a bill that would provide liability protection for companies that adopt advanced cybersecurity best practices. This may also include amending the Racketeering Influenced and Corrupt Organizations Act (RICO) to cover cybercriminals and hackers.

**Senate Proposal:**
While the House has always favored a piecemeal approach to address cybersecurity, the Senate continues to pursue a comprehensive bill, with several committees working to tie in the White House proposal with one piece of legislation, the Cybersecurity and Internet Freedom Act of 2011 (S. 413).

S. 413, introduced by Senators Lieberman (I-CT), Collins (R-ME) and Carper (D-DE), would establish a new office of cyberspace policy within the Executive Office of the President to oversee federal policies and activities on cybersecurity, working in conjunction with a new National Center for Cybersecurity and Communications within DHS. The bill authorizes the President, using the least disruptive means feasible, to declare cyber emergencies requiring "covered critical infrastructure" to implement mitigation plans. After much concern over this provision, the bill's authors clarified that the bill explicitly prevents the President from shutting down the Internet.

In its current form, the bill could suggest a heavy regulatory burden for major infrastructure operators. Certain sections of the bill establish potentially prescriptive risk-based performance regulations, as well as a supply chain risk-management strategy aimed at federal procurement.

S. 413 was referred to the Senate Homeland Security and Governmental Affairs Committee, where a hearing was held in May. Though there has been little legislative movement, this bill remains the Senate's foremost vehicle for addressing the nation's cybersecurity vulnerabilities.

**White House Proposal:**
In May, the White House released its cybersecurity legislative proposal. Similar to S. 413, the proposal authorizes DHS to establish risk-based performance standards for covered critical infrastructure (CCI). Covered infrastructures would be tiered based on criticality of assets,

similar to CFATS. Owners and operators of CCI would be required to develop risk mitigation plans, evaluated annually by a third party auditor, and they would need to certify with the SEC or DHS that their plans are sufficient.

The plan has received criticism for a provision requiring owners of CCI to publicly disclose summaries of their plans and evaluations. Although they can exclude proprietary information and vulnerabilities, stating publicly whether or not a company's cybersecurity plans are effective is counterproductive to good security. The Senate is likely to correct this measure as it incorporates the White House proposal into its own plan.

## Employee Background Check Restrictions

### Criminal History Checks:

At the Federal level, all eyes are on the Equal Employment Opportunity Commission (EEOC), where a Democratic majority is increasingly likely to revise the EEOC's longstanding guidelines for employers on the use of criminal background checks. Democratic Commission members, supported by "second chance" advocates, believe employment criminal background checks disproportionately impact minorities and could be considered discriminatory under Title VII of the Civil Rights Act. To lessen the impact of employee criminal checks on minorities, the Commission is considering revising its 1987 guidance to employers in ways that will restrict the use of the checks on current and prospective employees. Some possible changes are putting limits on the "look back" period for convictions, restricting when criminal checks can be conducted during the hiring process, and having different standards for current and prospective employees. EEOC guidance does not require a formal/public notice and comment period and some believe new guidance could be issued before the end of the year.

At the state and local level, an increasing number of states, counties and municipalities have enacted "ban the box" statutes in regard to their hiring practices (and, in some cases, those of government vendors) which ban questions about criminal history from initial written job applications. While only Hawaii, Massachusetts and the city of Philadelphia have extended the box ban to private employers, other states and cities are considering such measures.

### Credit Checks:

In July 2011, Connecticut became the sixth state to ban or limit the use of credit checks for employment purposes. The five other states with such laws are Maryland, Illinois, Washington, Oregon and Hawaii. The Connecticut law exempts financial institutions and makes exceptions in the cases where: a credit report is required by law, the employer reasonably believes that the employee has engaged in activity that is in violation of the law, or a credit report is "substantially related" to the employee's current or potential job. Similar legislation restricting the use of employee credit checks was introduced in 25 states in 2011.

At the Federal level, Democrats re-introduced the "Equal Employment for All Act" which would amend the Fair Credit Reporting Act to prohibit employers (with some exceptions) from using credit checks for employment purposes or making an adverse action. The bill has no chance of being passed by the GOP controlled House.

## Guns in the Workplace

There are now 20 states that have enacted various laws limiting the rights of employers to restrict employees from keeping guns in their vehicles while at work --- Alaska, Arizona, Florida, Georgia, Idaho, Indiana, Kansas, Kentucky, Louisiana, Maine, Minnesota, Mississippi, Montana, Nebraska, North Dakota, Ohio, Oklahoma, Tennessee, Texas, Utah and Wisconsin. Some of these laws even allow workers to sue their employers for even asking about firearms in vehicles. Other states are considering similar law and it seems that despite strong opposition from local business groups and statistics on workplace violence, Second Amendment rights are trumping property rights and workplace safety at every turn.

In related developments, in Texas and other states there are bills pending to allow students to carry concealed weapons on college campuses. Last year, Louisiana became the seventh state to pass a law allowing guns in places of worship. And many states have laws permitting (and others are powerless to stop) persons with concealed weapons permits from bringing guns into restaurants (including bars in some states).

## Data Breach Legislation

Despite great interest spurred by the massive 2011 data breaches at Sony and Epsilon, and with many possible legislative vehicles to choose from, Congress continues to struggle to get close to passing a federal data breach notification law that will replace the current patchwork of 47 state laws. One Republican vehicle, H.R. 2577 (the "Secure and Fortify Electronic Data Act") was passed by a House Energy and Commerce Subcommittee in late July. That bill, like others in Congress, would set a national standard for breach notification ("reasonable risk" data breach could lead to ID theft or fraud) and would require security measures to protect personal data. Democrats objected to the bill's limited definition of "personal information" and privacy groups complained its protections were too weak.

In the Senate, there are no less than four competing Democratic and bi-partisan proposals, including Sen. Patrick Leahy's Personal Data Privacy and Security Act (S.1151), Senator Rockefeller's Data Security and Breach Notification Act (S. 1207), Senator Dianne Feinstein's Data Breach Notification Act (S.1408), and Senator Tom Carper's Data Security Act (S. 1434). Additionally, in May the White House put forth a proposal for comprehensive cybersecurity and data breach notification legislation, and the data breach language is similar to that in the Leahy and Rockefeller bills.

Two of the Senate bills, Leahy (S.1151) and Feinstein (S. 1408) are scheduled for Judiciary Committee action in September. However, the Senate Commerce, Science and Transportation Committee also claims jurisdiction over data security, and that Committee is likely to move S. 1207 (introduced by Committee Chairman Rockefeller) in the near future.

As noted in earlier reports, while all the bills will create an national data breach notification standard, they may differ in triggering requirements for notification; definitions of "personal information"; obligations on data holders to protect data; the form and recipients of notice; timetables for providing notice; and remedies and penalties.

Most believe the prospects of data breach legislation passing both the House and Senate to be slim at best. The states are not waiting on Congress, though, and California and Illinois recently passed bills strengthening and expanding their current data breach laws.

## Suspicious Activity Reporting Programs and Legislation

Last year, DHS launched the "If You See Something Say Something" campaign to raise public awareness of indicators of terrorism and to emphasize the importance of reporting suspicious activity to the proper state and local law enforcement authorities. Since then, DHS has partnered with federal, state, municipal and private entities on the campaign, including the U.S. Chamber of Commerce, the NCAA, the American Hotel and Lodging Association and Walmart. In conjunction with the SSSS campaign, DHS and DOJ also started the Nationwide Suspicious Activity Reporting Initiative (NSI). The NSI is a partnership among federal, state, and local agencies to establish a national capacity for gathering, documenting, processing, analyzing, and sharing suspicious activity reports (SAR).

**ASIS Involvement:**
While the focus of the NSI is on law enforcement training and cooperation, as part of the NSI, DOJ is currently developing training material for its "non-traditional" partners (EMS, firefighters, 911 operators, parole officers) including the private sector (private security). Working off its "line officer" training video for law enforcement, DOJ is now developing, with input from ASIS members, an online training video/program for private security. The video will incorporate private security industry figures (Clyde Miller, Director of Corporate Security at BASF) and cover indicators and behaviors that would arouse suspicion in a reasonable person. The training will also describe the SAR process, and discuss privacy and civil liberty issues. The video could be completed by the end of the year.

**Federal Legislation:**
Congress has also become involved in supporting suspicious activity reporting with legislation to provide legal immunity to persons who report possible terrorist activity to authorities. In July, the House Judiciary Committee passed H.R. 963, the See Something Say Something Act, which was introduced by Judiciary Chairman Lamar Smith. A companion Senate bill was introduced by Senate Homeland Security Committee Chairman Joe Lieberman (I-CT) and Ranking Member Susan Collins (R-ME). The bill expands protections against lawsuits for good faith reporting to an "authorized official" (e.g. fed or law enforcement official) of all suspected terrorist related activity. Currently such protection is only provided for good faith reports of possible terrorist activity aimed at "passenger transportation systems." The bill covers reports of "any suspicious transaction, activity, or occurrence indicating that an individual may be engaging, or preparing to engage, in a violation of law relating to an act of terrorism."

The bill is not new. It was introduced in the 111th Congress by Rep. Peter King (R, NY-3rd), who also introduced a version in the 112th Congress (H.R. 495). Last Congress, however, under the Democratic controlled House and with liberal Rep. John Conyers (D, MI-14th) chairing Judiciary, it was never brought up. The prospects for the bill in the Senate are hard to discern at this time.

**Increased FBI checks on security officers: the Private Security Officer Employment Authorization Act (PSOEAA)**

In 2006, DOJ issued rules for states and employers to implement the PSOEAA. Since then, ASIS and NASCO have worked to get states not currently conducting FBI checks on security officers as part of a state licensing scheme or under a state statute to start doing so pursuant to the PSOEAA. Over the past eighteen months there has been some success, and now "authorized" employers of security officers (proprietary or contract) have the ability to request FBI checks for their officers in the states of Missouri, Colorado and Kentucky through PSOEAA programs set up by those states. In addition, through an "Alternate State" program set up by Minnesota, security officer employers can request from Minnesota state officials FBI checks on their officers in Alabama, Idaho, Kansas, Mississippi, Nebraska, South Dakota and Wyoming, and possibly others states.

Becoming an authorized employer is simply a matter of filing a certification statement with the state performing the check. A PSOEAA check entails screening an officer's state and FBI criminal history record information against reporting criteria in the PSOEAA (all felony convictions and convictions within 10 years for non-felony crimes involving ''dishonesty or a false statement'' or ''the use or attempted use of physical force''), and then notifying the employer as to whether the officer's record meets the criteria ("Yes" or "No"/"Meet" or "Does not Meet"). The process from the time the prints are received by the state until the result is provided is approximately eight days. The cost for a PSOEAA check is approximately $39.25 ($15 for the state check and $24.95 for the FBI check).

**PS PREP Program**

The Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep) was set up pursuant to the 9/11 Commission Recommendations Implementation Act of 2007. Congress directed DHS to develop and implement a voluntary program where private sector organizations may be certified by an accredited third party establishing that the private sector entity conforms to one or more comprehensive preparedness standards adopted by DHS. In June 2010, DHS formally adopted three standards for the program: ASIS International SPC.1-2009 Organizational Resilience; BSI 25999 Business Continuity Management and NFPA 1600 Disaster/Emergency Management and Business Continuity Programs (2007 and 2010 editions).

In September 2010, the ANSI-ASQ National Accreditation Board issued requirements and invited certification bodies to submit applications for accreditation for the PS-Prep program. Once accredited, certification bodes will issue certificates of conformance to organizations that

are found to comply with any or all of the three standards designated by DHS for the PS-Prep program. In October 2010, DHS requested comment on its small business plan for PS-Prep, which would allow for entities with fewer than 500 employees to certify via "self-declaration of conformity."

So far no companies have undergone the PS-Prep process, although FEMA officials running the program claim there are some large companies who have committed to becoming "early adopters." In late August, ANSI announced the accreditation of the International Consortium for Organizational Resilience (ICOR) under the ANSI Certificate Accreditation Program, making ICOR the first credentialing organization to achieve ANSI accreditation of its training programs for PS-Prep.

There is still much confusion over what exactly PS-Prep certification will mean to a company and what such certification will cover. There is also the issue of the cost of third party certification. While DHS continues to maintain that the program is voluntary, rumors continue to circulate (perhaps pushed by certification bodies) that PS-Prep certification could become a requirement for obtaining government contracts, or that the federal government will take other actions to push organization to adopt the program.

**Private Security Access/Credentialing for Disaster and Emergency Areas**

Access to disaster sites by non-emergency responders is a long-standing challenge that has been hard to resolve, in large part due to the vast number of jurisdictions involved at all levels of government nationwide. DHS is currently working with private sector groups, including security, on various efforts to address this issue. One forum is the DHS Emergency Services Sector Coordinating Council (ESSCC), the non-federal component of the Emergency Service Sector Committee, which is one of the 19 committees that make up the DHS Critical Infrastructure Partnership Advisory Council. Representing private security interests on the ESSCC are NASCO and Securitas. Other members on the ESSCC include: police, fire, EMS, public works, and emergency management organizations. The National Sheriffs Association is the primary driver on the ESSCC.

Another credentialing forum in which ASIS representatives participated was FEMA's "Building Resilience through Public-Private Partnerships" conference. During the forum there was a breakout session to discuss how to develop a system that local jurisdictions can use to govern the ability of the private sector to enter restricted areas without hindering the disaster response. The group determined that the key is to put together a system that can effectively provide credentialing ahead of time, and access just in time. While setting up a workable system will depend on many factors, it was suggested at the meeting that DHS assemble "Tools and Resources" that could aid government and private sector entities in dealing with the problem of access/credentialing.

Suggested items include: a nationally accessible collection of good practices from the private sector and government; an umbrella initiative to identify and connect existing efforts to resolve this issue; dedicated points of contact at the state/tribal/territorial/local levels who can maintain

the networks year-round and handle emergency requests; a reference catalogue of existing state regulations and authorities impacting access; sample enabling legislation from states that have put this in place; standards to provide general guidelines; and a collaborative web site, such as a Wiki, where the public and private sectors can post disaster site best practices related to access issues and work together to build newer, better solutions.

## FAA Rollback of Block Aircraft Registration Request (BARR) Program

In August, the Federal Aviation Administration put in place its plan to curtail the Block Aircraft Registration Request (BARR) program, which allowed general aviation operators to opt out of having their flight plans and en route data made publicly available. Approximately 7400 airplanes had their information blocked prior to the program change. The program was created in late 1990's and authorized by Congress in 2000 as a result of the rise of online flight tracking services that were seen as compromising individual security, privacy and business competitiveness. Under the new program rules, flight data can only be blocked if there is written certification of a valid security threat. Currently only 970 airplanes have met this standard.

The change of policy, in the name of "government transparency," is being fought by aviation groups, industry, and privacy groups. An aviation industry suit challenging the FAA's program change as "arbitrary and capricious" is currently in its briefing stages in the U.S. Court of Appeals in the D.C. District. Efforts to rollback the change also are underway in Congress. Most significantly, a provision was added to the House FAA reauthorization before it was passed that would preserve the BARR program. However, it is not known whether the provision will make into the final House/Senate FAA reauthorization conference report.

## SAFETY Act Updates

The Support Antiterrorism by Fostering Effective Technologies (SAFETY) Act, enacted by Congress as part of the Homeland Security Act of 2002, provides liability limitations for developers and users of "qualified anti-terrorism technologies" for claims arising out of, relating to, or resulting from an act of terrorism. SAFETY Act advocates claim that without the Act, numerous anti-terrorism products and services would not be in the marketplace. Such a claim is highly debatable, however, and the SAFETY Act's liability limitations have never been put to the test. Since the program began in 2004, approximately 450 products and services have received either SAFETY Act Designation or Certification as a "qualified anti-terrorism technology."

At a May House Homeland Security Committee hearing on the SAFETY Act, DHS reported that since 2006 it has cut the application processing time by 30% (to 113 days on average). There was concern that too many technologies were being denied "Certification" status, which provides greater liability protection than Designation status and also allows companies to advertise their approval status to customers. In addition, business groups complained that the lesser Designation is problematic for companies seeking insurance, as many insurers don't understand it.

The SAFETY Act program enjoys strong support in Congress, but the DHS Science and Technology budget, where the program is funded, was cut by 22% in FY 2011 and faces an even greater cut in FY 2012.

Recently, ASIS International was granted SAFETY Act Certification (thus, also Designation) for its Organizational Resilience Standard that was adopted by DHS in 2010 as a DHS National Standard as part of the PS-PREP program. The "technology" certified also "includes the standards development processes and procedures used by ASIS International to develop the named standard." This means that other ASIS Standards, developed using the same standard development process, could also obtain certification upon a showing that they have anti-terrorism applicability.

**Contact Information**

For more information on these or other federal legislative issues, contact:

Jack Lichtenstein, ASIS VP of Government Affairs & Public Policy: 703-518-1498 / jack.lichtenstein@asisonline.org

Kristin Rubin, ASIS Legislative Director: 703-518-1487 / kristin.rubin@asisonline.org

Steve Amitay, Amitay Consulting, LLC: 202.347.4805 / steve@amitayconsulting.com