Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

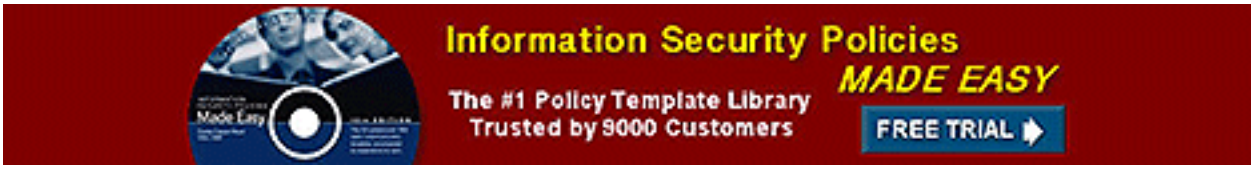
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The 2001 Patriot Act and Its Implications for the IT Security Professional

As part of the post-September 11th rush to protect America from acts of terror, the United States Government signed into law legislation that would give the government additional tools to help track, prevent, and combat terrorism. The controversial USA Patriot Act (USAPA) has garnered both support and contempt from Americans. Some describe its tenets as Draconian in scale while others criticize it as not doing enough to ensure the safety of US citizens. Regardless of one's view, the USAPA will likely have a significant...

Copyright SANS Institute
Author Retains Full Rights

AD



The 2001 Patriot Act and Its Implications for the IT Security Professional

Oscar W. Peterson III
GSEC Practical Version 1.3
February 16, 2002

Abstract

As part of the post-September 11th rush to protect America from acts of terror, the United States Government signed into law legislation that would give the government additional tools to help track, prevent, and combat terrorism. The controversial USA Patriot Act (USAPA) has garnered both support and contempt from Americans. Some describe its tenets as Draconian in scale while others criticize it as not doing enough to ensure the safety of US citizens. Regardless of one's view, the USAPA will likely have a significant impact on the IT Security Professional (ITSP).

One could write volumes of encyclopedic magnitude discussing the ethical and moral implications of the USAPA. One could also spend an equal amount of time delving into criticism and the Big Brother implications of this law. However, for the purpose of this paper, such things will be out of scope. Instead, the paper will focus on IT related issues encompassed by the USAPA in general as well as possible actions that could be expected of ITSPs. The ultimate goal of this paper will be to provide the ITSP with a broad understanding of the IT related sections of the USAPA and how it might impact his or her work environment.

For the duration of this paper, information in quotations is taken directly from H.R. 3162-USAPA unless otherwise notated.

USAPA In Brief

Decried by many as an Orwellian nightmare, the 342 page "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" or USAPA was signed into law on October 26, 2001, five weeks from its initial introduction. It passed overwhelmingly with a vote of 357-66 in the House of Representatives and 98-1 in the Senate. Proponents of the Law praise it as a necessary step in the government's fight to protect Americans and in the American's right to feel safe from terrorism. Opponents criticize it as being government friendly, socialist, and too invasive. On the surface the majority of the USAPA makes modifications of varying degrees to many preexisting laws regarding immigration, surveillance, victim compensation, money laundering, and intelligence gathering and sharing. At its heart the USAPA grants additional powers to law enforcement and intelligence agencies, both international and domestic, while removing many of the obstacles that were formerly in place.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

USAPA Implications for the IT Security Professional

The USAPA begins with **Title I-Enhancing Domestic Security Against Terrorism** and wastes no time establishing that the US Government is taking cyber terrorism very seriously. **Section 103** calls for an additional $600,000,000 in funding for the FBI's Technical Support Center to be evenly dispersed over three years (2002, 2003, 2004). This significant monetary investment will almost certainly increase the frequency in which the government requests data, facilities, and other assistance from ITSPs and their companies. These additional funds will also likely be used for creating new IT Security jobs with the FBI, thus increasing the potential job market for existing ITSPs.

Section 105 orders the expansion of the nation's electronic crime task force "for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems." This expansion will mean the creation of many new jobs in IT Security. As the number of jobs increases, so will the frequency and quality of training available to those interested in IT Security.

While **Title I** establishes a baseline for the creation of additional resources for government-based IT Security, **Title II-Enhanced Surveillance Procedures** establishes the operational guidelines by which information can be gathered. It is also the most relevant section to the ITSP. This section improves upon and clarifies previous law. The Computer Fraud and Abuse Act (CFAA) and the Foreign Intelligence Surveillance Act (FISA) are both heavily modified and elucidated in this section.

Title II begins by clarifying the authority of government agencies to "intercept wire, oral, and electronic communications." It is important to note that the section dealing with computer fraud and abuse (**Section 202**) immediately follows a section dealing with terrorism (**Section 201**). The proximity of these two items serves to reinforce the fact that the government is taking actions that threaten the security of our computers and networks just as seriously as those acts traditionally known to us as terrorism (i.e. a suicide bomber in a crowded shopping center). This will become even more evident in the discussion on **Title VIII-Strengthening the Criminal Laws Against Terrorism** later in this paper.

Section 203 grants government agencies a much greater ability to share investigative information across what used to be barriers in jurisdiction. It states that law enforcement, with knowledge obtained by "…electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official." The fact that it is now much easier for government agencies to share information will likely increase the frequency of which electronic information is requested by the government. The increase in governmental requests is certain to add to the ITSP's workload provided that the ITSP's help is even requested. Fortunately, the USAPA makes provisions for reasonable compensation when the assistance of a civilian ITSP is needed (**Section 222**).

Section 206 increases the ability of the government to track persons who attempt to disguise their identity. For example, evidence of a person who frequently changes their ISP in an attempt

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

to avoid surveillance would be easier to obtain, as many boundaries of jurisdiction would be gone. It is possible that the government could ask an ITSP working for one ISP for information regarding their customers, and then compare that information with information gathered from other ITSPs to determine patterns and track abnormal ISP switching. It's becoming increasingly important for companies and their ITSPs to keep accurate and up-to-date records of activities of persons utilizing their services.

The USAPA also makes it much easier for the government to obtain electronic information. **Section 209** changes a previous law that required the government to obtain both a warrant and a Title III wiretap order to gain access to stored voicemail. Under this new section, the government can gain this type of access with a simple search warrant. Increases in the frequency of government requests for electronic information will most likely result. This could, in turn, increase the workload of ITSPs.

Section 210 expands the types of information that the government can subpoena from companies. Under the new law the government can request information regarding the duration of sessions and the times those sessions occurred. **Section 210** also includes information regarding temporary network addresses. Furthermore, the government is able to request lengths of service (i.e. with specific ISPs – in this way this section coincides with **Section 206** regarding tracking of users who change ISPs to avoid law enforcement). Additionally, the government can request information about a customer's method of payment for their Internet service, including bank accounts, credit card information, or other means of payment for the service. It is important to note here that the government can only request this type of financial information as it relates to the Internet service itself. This provision does not include information used to make online purchases (unless the online purchase was for Internet service) or information stored in online wallets or digital passports.

Section 211 makes it possible for cable companies to provide customer information to the government without notifying the customer. This change modifies a previous Cable Act provision that required companies notify their customers of government inquiries. Of course this situation is very beneficial to cable companies, as they will not have to deal with bad press and customer complaints resulting from the handing over of data to the government. Cable companies that are able to cooperate with government requests without the fear of negative backlash from their customers may make them more apt to cooperate. This fact will also likely cause an increase in the workload of the ITSP as government requests for information. Here again we see the importance of a company's ITSP's record keeping habits.

Section 212 states that "emergency disclosure of electronic communications" in cases where there is a reasonable threat of "danger of death or serious physical injury to any person" is allowed. In fact, the section goes on to say that in these cases disclosure of said information is required "without delay." This change underscores the importance that the ITSP not only keeps thorough and accurate records but that he or she is very aware of the data that is passing through his or her company's network and that they know how to respond immediately if a situation arises.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Section 214 broadens the scope of information that can be retrieved via pen registers and trap and trace devices. Previously, information gathered in this manner had to be directly linked to involvement in terrorist activities. After the USAPA the information has to be "relevant" to an ongoing investigation. This change aligns pen register and trap and trace information gathering with the Electronic Communications Privacy Act (ECPA). It's not very likely that an ITSP would be tasked with the gathering of pen register and track and trace information. However, it is important for the ITSP to be familiar with the legal ramifications of these types of data collecting methods in case the need arises.

Section 215 expands the list of items that can be subpoenaed by the government for terrorism investigations. The FBI can instigate an order that "requires the production of any tangible things (including books, records, papers, documents, and any other items)." The ITSP should note that this provision encompasses *any* "tangible things." Of course, among this category are servers, hard drives, diskettes and a myriad of other items under the watchful eye of the ITSP. Again, we see the need for the ITSP to maintain detailed records of equipment and access.

This section also makes it clear that the ITSP should not reveal the purpose of the gathering of these "tangible things" to anyone who is not specifically needed to "produce the tangible things" or that the FBI has sought them. Furthermore, this section states that any person (in our case the ITSP) "shall not be liable to any other person" for the production of any items included under the moniker of "tangible things." In short, the ITSP must keep any details of an investigation secret, and he or she need not fear litigious action if involved in producing any items needed by the FBI for their investigation.

By including "routing" and "addressing," **Section 216** clarifies that pen register and trap and trace information gathering includes Internet traffic. It also states that once an order under this provision is issued it "shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order." ITSPs should note that once an order has been issued law could require them to assist the government in its investigation. This section also includes a provision whereby the ITSP may request a written statement, which the government must provide, detailing his or her inclusion in the investigative order.

Additionally, this section sets up some ground rules for the government's use of pen register and trap and trace devices on "packet-switched networks." *Carnivore*, a technology introduced by the FBI that can monitor and record all Internet traffic going into and out of an ISP, has recently received a lot of press. This technology is most likely what lawmakers had in mind at the time of this section's writing (Olsen). Any law enforcement or government agency that utilizes *Carnivore* (or similar technology) to acquire data must provide detailed reports including: any officers who installed or accessed the device; dates and times of the technology's installation and uninstallation; dates, times, and durations of each time the technology was accessed for information; the configuration of the technology at the time of installation; and any other modifications to the technology during its use, and any information that was collected by the device.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Ultimately, **Section 216** will increase the frequency of the government's Internet traffic monitoring requests. This section will do so by effectively removing boundaries of jurisdiction for per register and trap and trace technologies. When such an order is issued it immediately becomes applicable across all states and jurisdictions. The ITSP must remember that an order issued in any state applies to his or her company anywhere else United States law is applicable.

Section 217 defines the "computer trespasser" and offers the government protection against litigation if it participates in warrant-less searches at the request of the owner of the "protected computer." The ITSP should be aware of what the government defines as a "computer trespasser." Basically, a "computer trespasser" is a person who engages in unauthorized access of a "protected computer." This section goes on to state that such individuals have "no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer." Furthermore, this section gives the government the ability to intercept the electronic communications of a "computer trespasser" without a warrant. As long as the owner or operator of the "protected computer" authorizes the interception, the government remains within the limits of the law.

Section 218 could also increase the frequency of the government's requests for electronic information. This section relaxes some of the FISA standards regarding foreign intelligence gathering, subsequently making it easier for the government to issue orders of this type. Previously, the FISA provision was that, in order for the government to issue an order for the gathering of foreign intelligence, the information under suspicion had to be "the purpose" for the surveillance. With the modifications made by this section, the information under suspicion can be "a significant purpose" for the surveillance. Basically, the government now needs probable cause rather than proof to issue orders for search or surveillance in foreign intelligence matters.

This section is primarily significant for ITSPs working in companies that provide employees with Internet access. In this type of environment, ITSPs may be expected to provide logs of electronic communications if the government suspects that the information may be involved in some sort of foreign terrorist activities. Now that the government only needs to prove that the information is significantly related to suspicious foreign activities, requests for this data are likely to increase.

Section 219 and **Section 220** make it easier for the government to get nationwide search warrants to assist in investigations involving both domestic and international acts of terrorism. These sections set things up so that a warrant issued in one jurisdictional area will be applicable to any other area where US law is enforced, negating previous requirements that the government obtain warrants for separate jurisdictional areas in which terrorism is suspected. With the increased ease by which the government can obtain warrants and issue orders, companies and ITSPs will likely have to deal with the increase in requests for information, personnel, or facilities. It is also likely that ITSPs may be enlisted in these searches.

Fortunately, the increased workload and expectations of ITSPs and companies brought about by the USAPA will not legally require the acquisition of additional equipment or other resources. **Section 222** states: "Nothing in this Act shall impose any additional technical obligation or requirement on a provider of a wire or electronic communication service or other person to

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

furnish facilities or technical assistance." This section emphasizes the fact that previously existing provisions in regards to the assistance expected of companies (and ITSPs) will remain the same and states that the government will not legally require companies to purchase additional expertise or equipment to help in an investigation. This section goes on to say that any service provider or other entity or person who provides technical assistance, "pursuant to section 216," will be "reasonably compensated" for their "reasonable expenditures" related to the investigation.

Section 223 gives protection to the federal government against lawsuits. ITSPs should note that there are some checks and balances in place for improper behavior of government officials. While the government cannot be taken to court, this section does have provisions for litigious action against government and investigative officials who improperly disclose information obtained during an investigation. The intention of this section is to keep government officials accountable for their actions and to keep information gathered during an investigation confidential.

Many of the sections of **Title I** and **Title II** of the USAPA have a "sunset" provision. **Section 224** states that many of these sections will expire on December 31, 2005. The text of this section is as follows:

> (a) IN GENERAL- Except as provided in subsection (b), this title and the amendments made by this title (other than sections 203(a), 203(c), 205, 208, 210, 211, 213, 216, 219, 221, and 222, and the amendments made by those sections) shall cease to have effect on December 31, 2005.
>
> (b) EXCEPTION- With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in subsection (a) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect. (USAPA).

The above items are the exceptions to the "sunset" provision of the USAPA's **Title I** and **II**. It is not in the scope of this paper to relate these exceptions in detail as all of the provisions of the USAPA are currently in effect and can presently impact the work environment of the ITSP.

Section 225 provides immunity for "any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnished any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act." Basically, ITSPs cannot have legal action taken against them for complying with a court order in regards to a FISA wiretap.

Title III through **Title VI** deals with financial issues in regards to terrorism, border protection, removing investigation obstacles, and victim compensation respectively. These sections might have a minimal impact on ITSPs in very specific areas (banking,

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

INS, educational facilities). Since the purpose of this paper is to provide a broad view of the impact of the USAPA on ITSPs in general, it will not delve into these sections.

Title VII Section 701 calls for the expansion of information sharing systems. The government will authorize $150,000,000 over the years 2002 and 2003 to "establish and operate secure information sharing systems." This will be done to improve multi-jurisdictional investigations and will very likely create an increase in demand for qualified ITSPs for the systems' configuration, implementation, operation, and maintenance.

Title VIII strengthens criminal laws against terrorism, clarifies definitions of domestic terrorism, and discusses penalties for terrorist acts. Most important to the ITSP is **Section 814**. This section, entitled Deterrence and Prevention of Cyberterrorism, clarifies penalties for hacking and expands the authority of law enforcement and other government agencies in dealing with cyber-terrorism.

In defining cyber terrorist offenses, this section states that an offense is prosecutable if the action taken (or the result of attempted action if completed) meets any of the following:

> `(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
>
> `(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
>
> `(iii) physical injury to any person;
>
> `(iv) a threat to public health or safety; or
>
> `(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;'. (USAPA).

This section demonstrates the necessity of the ITSP to keep current and accurate records. In order for the government to prosecute a hacker, one or more of the aforementioned points will have to be proven. The best way for this to be done is through comprehensive and accurate record keeping on the part of the ITSP. It's also important for the ITSP to understand that in calculating damage costs he or she should also include costs related to response, restoring data, damage assessments, interruptions (denials) of service and recovery.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Furthermore, (much to the benefit of many software designers) this section states that civil action cannot be brought against anyone for "negligent design or manufacture of computer hardware, computer software, or firmware."

Section 816 authorizes $50,000,000 for the creation and support of regional computer forensic laboratories. These facilities will not only be expected to conduct cyber-security forensics but they will also be centers for training and education of Federal, State and local law enforcement personnel as well as legal teams who are prosecuting cyber-terrorism cases. These labs will also facilitate communication between the Federal, State, and local levels in issues regarding cyber-security forensics. The creation of these facilities will contribute to the increase in the ITSP job market.

Title X Section 1005 provides grants to "first responders" (i.e. State and local law enforcement, fire departments) in regards to preventing terrorist activity. The grants fall under two categories: Terrorism Prevention and Antiterrorism Training.

Terrorism Prevention grants will be used to:

> (1) hire additional law enforcement personnel dedicated to intelligence gathering and analysis functions, including the formation of full-time intelligence and analysis units;
>
> (2) purchase technology and equipment for intelligence gathering and analysis functions, including wire-tap, pen links, cameras, and computer hardware and software;
>
> (3) purchase equipment for responding to a critical incident, including protective equipment for patrol officers such as quick masks;
>
> (4) purchase equipment for managing a critical incident, such as communications equipment for improved interoperability among surrounding jurisdictions and mobile command posts for overall scene management; and
>
> (5) fund technical assistance programs that emphasize coordination among neighboring law enforcement agencies for sharing resources, and resources coordination among law enforcement agencies for combining intelligence gathering and analysis functions, and the development of policy, procedures, memorandums of understanding, and other best practices. (USAPA).

Antiterrorism Training grants will be used for:

> (1) intelligence gathering and analysis techniques;
>
> (2) community engagement and outreach;
>
> (3) critical incident management for all forms of terrorist attack;

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

(4) threat assessment capabilities;

(5) conducting followup investigations; and

(6) stabilizing a community after a terrorist incident. (USAPA).

This section further shows that the need for qualified ITSPs to train and assist Federal, State, and local agencies will be greatly increase as a result of the USAPA. Additionally, this section demonstrates that not all provisions of this Act translate into additional workload for the ITSP.

Conclusion

As a result of the USAPA, ITSPs will likely be expected, but not required, to be more diligent in keeping accurate records in order to provide the government with information when necessary. We have also seen that the workload of many ITSPs may be increasing as the government continues to crack down on cyber-terrorism. The increased governmental emphasis on IT Security will have a wide ranging impact on the IT Security Professional. Additional funds will create more and better paying jobs and are almost certain to increase the quality and availability of IT Security training programs. It is also very likely that the government's attention on IT Security will prompt the private sector to increase their security budgets and maybe even salaries for ITSPs.

In the global marketplace, opportunities for malicious behavior on US computer systems abound. Both the increasing speed and availability of information brought by the Internet, and the infusions of many different cultural and political agendas into corporations are factors in making today's networks and Internet risky but rewarding places to do business. Many of the new powers bestowed upon the government via the USAPA will impact the sphere of ITSPs. The US Government and various law enforcement agencies will likely shoulder most of the burden for the implementation of the USAPA. However, there are many possible actions that may be expected of ITSPs, and we should be read to assist.

List of References

"EFF Analysis Of The Provisions Of The USA PATRIOT Act." EFF Analysis of USA PATRIOT Act. 31 October 2001. URL: http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html (28 Jan. 2002).

"Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001." Computer Crime and Intellectual Property Section. 5 November 2001. URL: http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm (28 Jan. 2002).

"Federal Statutes Related to Searching and Seizing Computers: Redline Showing Changes Resulting from 2001 USA Patriot Act." Computer Crime and Intellectual Property Section. 19

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

December 2001. URL: http://www.usdoj.gov/criminal/cybercrime/usapatriot_redline.htm (28 Jan. 2002).

Garretson, Cara. "Ashcroft has Immediate Plans for Antiterrorism Tools." 25 October 2001. URL: http://www.computerworld.com/cwi/community/story/0,3201,NAV65-663_STO65051,00.html (7 Feb.2002).

"H.R. 3162." 24 October 2001. URL: http://www.epic.org/privacy/terrorism/hr3162.html (28 Jan. 2002).

Herman, Susan. "The USA Patriot Act and the US Department of Justice: Losing Our Balances?" 3 December 2001. URL: http://jurist.law.pitt.edu/forum/forumnew40.htm (7 Feb. 2002).

Olsen, Stephanie. "Patriot Act Draws Privacy Concerns." 26 October 2001. URL: http://news.com.com/2100-1023-275026.html?legacy=cnet (28 Jan. 2002).

Plesser, Ron. Halpert, Jim. Cividanes, Milo. "Summary and Analysis of Key Sections of the USA Patriot Act of 2001." Response to Sept. 11, 2991 Terrorist Attacks. 31 October 2001. URL: http://www.cdt.org/security/011031summary.shtml (10 Feb. 2002).

Raimondo, Justin. "It Can Happen Here." Antiwar.com: Behind the Headlines. 26 November 2001. URL: http://www.antiwar.com/justin/j112601.html (28 Dec. 2001).

"USA Patriot Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances." ACLU Legislative Analysis on USA Patriot Act. 1 November 2001. URL: http://www.aclu.org/congress/l110101a.html (28 Jan. 2002).

"USAPA Sunset Provisions Could Leave Congress in the Dark." EFF USAPA Sunset Analysis. 12 December 2001. URL: http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011212_eff_usapa_sunset_analysis.html (28 Jan. 2002).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: October 9th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Tysons Corner 2015	**Tysons Corner, VAUS**	**Oct 12, 2015 - Oct 17, 2015**	**Live Event**
SANS Gulf Region 2015	**Dubai, AE**	**Oct 17, 2015 - Oct 29, 2015**	**Live Event**
SANS Tokyo Autumn 2015	**Tokyo, JP**	**Oct 19, 2015 - Oct 31, 2015**	**Live Event**
SANS Cyber Defense San Diego 2015	**San Diego, CAUS**	**Oct 19, 2015 - Oct 24, 2015**	**Live Event**
SANS South Florida 2015	**Fort Lauderdale, FLUS**	**Nov 09, 2015 - Nov 14, 2015**	**Live Event**
SANS Sydney 2015	**Sydney, AU**	**Nov 09, 2015 - Nov 21, 2015**	**Live Event**
SANS London 2015	**London, GB**	**Nov 14, 2015 - Nov 23, 2015**	**Live Event**
Pen Test Hackfest Summit & Training	**Alexandria, VAUS**	**Nov 16, 2015 - Nov 23, 2015**	**Live Event**
SANS Hyderabad 2015	**Hyderabad, IN**	**Nov 24, 2015 - Dec 04, 2015**	**Live Event**
SANS San Francisco 2015	**San Francisco, CAUS**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
SANS Cape Town 2015	**Cape Town, ZA**	**Nov 30, 2015 - Dec 05, 2015**	**Live Event**
Security Leadership Summit & Training	**Dallas, TXUS**	**Dec 03, 2015 - Dec 10, 2015**	**Live Event**
SANS Cyber Defense Initiative 2015	**Washington, DCUS**	**Dec 12, 2015 - Dec 19, 2015**	**Live Event**
SOS: SANS October Singapore 2015	**OnlineSG**	**Oct 12, 2015 - Oct 24, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**