# National Insider Threat Special Interest Group (NITSIG)

## Legal Counsel Support To Insider Threat Program

**Legal Counsel Responsibilities**

- Advises the Insider Threat Program (ITP) Manager.
- Reviews proposed data collection techniques, use of data, and procedures undertaken in the conduct of insider treat inquiries and investigations.
- Reviews current and proposed ITP policy and procedures to ensure compliance with regulations, rules, laws.

**Protection of Employee Civil Liberties And Privacy Rights**
**Ensuring Compliance With Legal Mandates**

- Each organization should build their ITP working side-by-side with Legal Counsel and Privacy Officers.
- Members of organizational management, the ITP Manager, ITP Team and Legal Council must be familiar with existing legal mandates, statutes, and directives related to ITP implementation as well as privacy and civil liberties law.
- This familiarity helps to ensure that the program meets all legal requirements and actions, such as those related to user monitoring, confidential reporting, and protecting employee rights.
- The ITP Manager, ITP Team and supporting personnel must ensure that inquiries, investigations, actions and decisions are handles in accordance with privacy and civil liberties laws. The ITP Concept of Operations (CONOPS) should outline "The Lanes In The Road" for all individuals that manage or support the ITP.

**Privacy And Civil Liberties Rules, Regulations, And Laws -1**
**The Bill of Rights**

- Protects against unreasonable searches and seizures.
- Protects rights such as freedom of speech and assembly as laid out in the DoD Civil Liberty Principles and by statute The Privacy Act of 1974.
- Establishes safeguards to protect information collected about individuals - The Electronic Communications Privacy Act.
- Requires compliance with prohibitions and exceptions to interception, access, and disclosure of electronic communications - The Rehabilitation Act of 1973.
- Ensures that practices do not discriminate against an individual with a disability.

**Privacy and Civil Liberties Rules, Regulations, and Laws -2**
**Title VII Of The Civil Rights Act Of 1964**

- Ensures that practices do not discriminate based on race, color, religion, sex, or national origin Civil Liberties Principles.
- Require compliance with the prohibition of maintaining information on individuals who exercise their First Amendment rights.
- Protect civil liberties "to the greatest extent possible" Prohibited Personnel Practices.
- Ensure that prohibited actions, such as discrimination and nepotism, do not occur during personnel decision.

# LAWS

| NAME | DESCRIPTION |
|---|---|
| **Espionage** | Defined under Sections 792-799, Chapter 37, title 18, United States Code<br>Article 106a, Uniform Code of Military Justice (UCMJ) (reference: Section 801-940,<br>Chapter 47, of title 10, United States Code, Uniform Code of Military Justice) |
| **Title 18, USC 793** | Gathering, transmitting, or losing defense information |
| **Title 18, USC 794** | Gathering or delivering defense information to aid a foreign government. |
| **Title 18, USC 798** | Disclosure of classified information. |
| **Section 811, 1995 Intelligence Authorization Act** | Immediate notification to the FBI whenever there are indications that classified information may have been disclosed without authorization to a foreign power (non-DoD). |
| **Article 106a, UCMJ, Espionage (Title 10, USC Section 906a)** | Espionage by a member of the U.S. military. Not required to adhere to Section 811, 1995 Intelligence Authorization Act. |
| **Section 922, 2012 National Defense Authorization Act** | The DoD is required to establish a program for information-sharing protection and insider threat mitigation for all DoD systems. |
| **Executive Order #13587** | This Executive Order is intended to improve the security of classified information in government computer networks as part of the government's response to WikiLeaks. EO is supposed to reduce the feasibility and likelihood of the unauthorized release of classified information. It addresses gaps in policy for information systems security, including characterization and detection of insider threats |
| **Computer Fraud And Abuse Act (CFAA) (Title 18 USC § 1030(a)(4))** | Provides for civil and criminal remedies against any person who "knowingly and with intent to defraud, accesses a computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value."<br>18 U.S.C. § 1030(a)(4) |
| **RICO Act (Title 18 USC § 1961 et seq.)** | Pattern of Racketeering" requires two or more predicate acts such as mail/wire fraud, false statements, interstate transport of stolen goods, criminal copyright infringement.<br>Enterprise" includes any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity.<br>"Injured in his business or property" requires actual, quantifiable injury to business or property. |

| | |
|---|---|
| **Espionage** | Defined under Sections 792-799, Chapter 37, title 18, United States Code (reference: Sections 792-799, Chapter 37 of title 18, United States Code) and Article 106a, Uniform Code of Military Justice (UCMJ) (reference: Section 801-940, Chapter 47, of title 10, United States Code, Uniform Code of Military Justice) |
| **Espionage Act Of 1917 (18 USC § 792)** | The Espionage Act, passed in 1917 after the United States entered the World War I, prohibited the disclosure of government and industrial information regarding national defense. The act also criminalized refusal to perform military service if conscripted. It prohibited any attempt to interfere with military operations, to support U.S. enemies during wartime, to promote insubordination in the military, or to interfere with military recruitment. The law was further strengthened by the Espionage and Sabotage Act of 1954, which authorized the death penalty or life imprisonment for espionage or sabotage in peacetime as well as during wartime. The Act requires agents of foreign governments to register with the U.S. Government. It also suspended the statue of limitations for treason. In 1958, the scope of the act was broadened to cover Americans engaged in espionage against the U.S. while overseas. |
| **Economic Espionage Act (EEA) Of 1996** | In an effort to safeguard our nation's economic secrets, EEA was signed into law on October 11, 1996. It dealt with a wide range of issues, including not only industrial espionage (e.g., the theft or misappropriation of a trade secret and the National Information Infrastructure Protection Act). |
| **National Stolen Property Act (Title 18 USC § 2314)** | **Violation Requires**:<br>**1)** Transportation in interstate or foreign commerce of **2)** Goods, wares, or merchandise **3)** That the defendant knew were stolen, converted or taken by fraud. |
| **Title 18 USC § 1831 - Economic Espionage** | **(a)** In General.— Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—<br>**(1)** steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;<br>**(2)** without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;<br>**(3)** receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without |

| | |
|---|---|
| | authorization;<br>**(4)** attempts to commit any offense described in any of paragraphs (1) through (3); or<br>**(5)** conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,<br>shall, except as provided in subsection (b), be fined not more than $5,000,000 or imprisoned not more than 15 years, or both.<br>**(b)** Organizations.— Any organization that commits any offense described in subsection (a) shall be fined not more than the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided. |
| **Trade Secrets, Title 18 USC, Section 1832** | Theft of trade secrets is **(1)** whoever knowingly performs targeting or acquisition of trade secrets or intends to convert a trade secret to **(2)** knowingly benefit anyone other than the owner. Commonly referred to as industrial espionage |

## REGULATIONS

**Compliance Violations**

- Today's business world is more complex and interconnected than ever before. Private investors and institutions make major decisions about how they allocate their investments based on corporate earnings reports and other financial and management information provided by businesses.
- If that data cannot be trusted, the investment markets will not function. It was not long ago that names such as Enron, Adelphia, and WorldCom became almost synonymous with corporate accounting scandals. To prevent a repeat of such corporate management failures, regulations were created to require firms not only to provide accurate information but also to protect the information systems that manage corporate accounts.
- The best known of these regulations that also have consequences for **insider abuse incidents** are:
  - HIPAA
  - Payment Card Industry (PCI) Data Security Standards (DSS)
  - Sarbanes Oxley (SOX)
  - GLBA

Each of these address different types of protections which may be violated during **insider abuse incidents**.

## HIPAA

- HIPAA defines levels of protection that need to be in place when managing, distributing, or storing protected health information. These regulations apply to businesses in the healthcare industry and include hospitals, clinics, doctor's offices, health insurance companies, and healthcare clearinghouses.
- The regulation covers what types of healthcare information are considered private and who it can be disclosed to.
- Another part of the regulation specifies administrative, physical, and technical safeguards required for business processes and information systems used to process protected healthcare information.
- Penalties for violations can be as high as $1.5 million per violation.

## PCI DSS

The PCI DSS is an industry regulation specifying security controls to mitigate the risk of credit card fraud and information theft. The regulations include policies on:

- Maintaining a secure network
- Protecting cardholder data when stored or transmitted
- Implementing a vulnerability management program to maintain systems security
- Implementing access control methods to limit access to cardholder data
- Monitoring network and systems and testing them regularly

- As this is an industry standard, there are no government penalties for violations, but businesses that fail to comply may suffer restrictions on their use of payment card services.
- The failure to comply with PCI regulations may also indicate failure to comply with government regulation, which in turn, could result in fines and penalties.

## SOX

SOX was passed in direct response to corporate accounting scandals. Much of the regulation addresses corporate governance and financial reporting. One section is of particular interest to IT professionals: Section 404. Section 404 regulates the need for **internal controls** over how financial data is collected, managed, and reported.

**Companies Are Responsible For**:

- Having controls in place to prevent misstatements on financial reports
- Risk assessment with regards to information management systems
- Controls on the financial reporting process

Obviously, if **insiders** are able to manipulate internal records, commit fraud, and hide their activities, controls are insufficient to protect the integrity of a company's financial system.

## GLBA

- GLBA applies to financial institutions and includes protections for consumer privacy.
- Financial institutions are required to provide customers with details on what information is collected, how it is shared with other institutions, and what safeguards are in place to protect that information.

**Requirements Include:**

- Access controls on systems containing customer data
- Use of encryption
- Physical access controls
- Monitoring for abuse, attacks, and intrusion
- Incident response plans

**Contact Information:**
**Jim Henderson, CISSP, CCISO**
**Founder / Chairman Of The National Insider Threat Special Interest Group**
**CEO Insider Threat Defense, TopSecretProtection.Com, Inc.**
**Counterespionage-Insider Threat Program Training Course Instructor**
**Cyber Security-Information System Security Program Management Training Course Instructor**
**Cyber Threat-Insider Threat Risk Analyst / Risk Mitigation Specialist**
**888-363-7241 / 561-809-6800**
**Websites / E-Mail Addresses:**
**www.nationalinsiderthreatsig.org**
**jimhenderson@nationalinsiderthreatsig.org**
**www.insiderthreatdefense.com**
**jimhenderson@insiderthreatdefense.com**