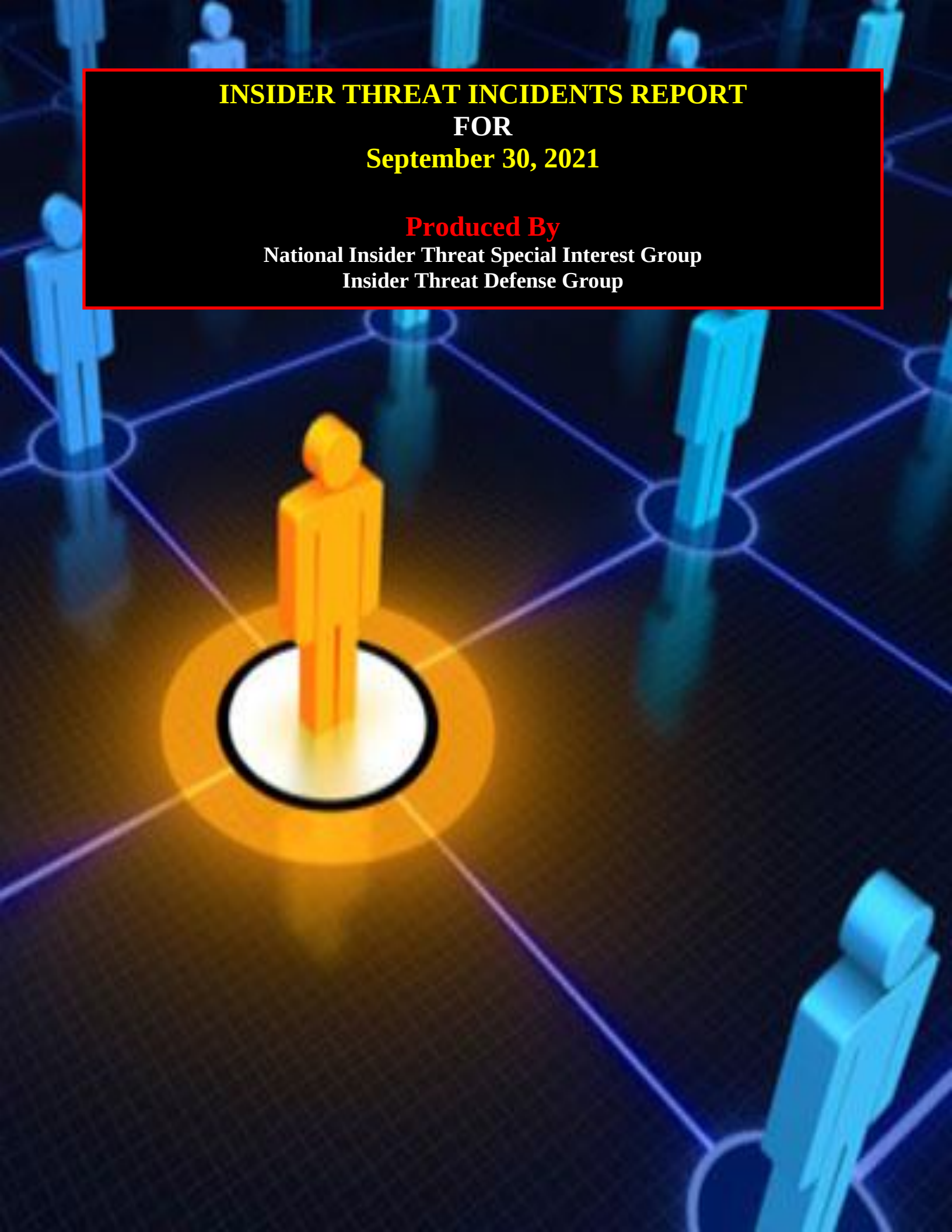

INSIDER THREAT INCIDENTS REPORT
FOR
September 30, 2021

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

INSIDER THREAT INCIDENTS

A Very Costly And Damaging Problem

For many years there has been much debate on who causes more damages (Insiders Vs. Outsiders). While network intrusions and ransomware attacks can be very costly and damaging, so can the actions of employees who sit behind firewalls or telework through firewalls. Another problem is that Insider Threats lives in the shadows of Cyber Threats, and does not get the attention that is needed to fully comprehend the extent of the Insider Threat problem.

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 10+ years. This research has evaluated and analyzed over **2,900** Insider Threat incidents in the U.S. and globally, that have occurred at organizations and businesses of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents, and receive a great deal of praise for publishing these incidents on a monthly basis to our various websites. This research provides interested individuals with a "***Real World***" view of the how extensive the Insider Threat problem is.

The traditional norm or mindset that Malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. Over the years there has been a drastic increase in financial fraud and embezzlement committed by employees.

According to the Association of Certified Fraud Examiners 2020 Report to the Nations, organizations with less than 100 employees suffered larger median losses than those of larger companies.

To grasp the magnitude of the Insider Threat problem, one most look beyond Insider Threat surveys, reports and other sources that all define Insider Threats differently. How Insider Threats are defined and reported is not standardized, so this leads to significant underreporting on the Insider Threat problem.

Another problem is how surveys and reports are written on the Insider Threat problem. Some simply cite percentages of how they have increased and the associated remediation costs over the previous year. In many cases these surveys and reports only focus on the technical aspects of an Insider stealing data from an organization, and leave out many other types of Insider Threats. Surveys and reports that are limited in their scope of reporting do not give the reader a comprehensive view of the "***Actual Malicious Actions***" employees are taking against their employers.

If you are looking to gain support from your CEO and C-Suite for detecting and mitigating Insider Threats, and want to provide them with the justification, return on investment, and funding ($$$) needed for developing, implementing and managing an ITP, the incidents listed on pages 5 to 22 of this report should help. The cost of doing nothing, may be greater then the cost of implementing a comprehensive Insider Threat Mitigation Framework.

DEFINITIONS OF INSIDER THREATS

The definition of Insider Threats can be vast, and must go beyond current definitions (By Sources Such As: National Insider Threat Policy, NISPOM CC2 & Other Sources) and be expanded.

While other organizations have definitions of Insider Threats, they can also be limited in their scope.

TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ Non-Malicious But Damaging Insiders (Un-Trained, Careless, Negligent, Opportunist, Job Jumpers, Etc.)
- ☐ Disgruntled Employees Transforming To Insider Threats
- ☐ Theft Of Organizations Assets
- ☐ Theft / Disclosure Of Classified Information (Espionage), Trade Secrets, Intellectual Property, Research / Sensitive - Confidential Information
- ☐ Stealing Personal Identifiable Information For The Purposes Of Bank / Credit Card Fraud
- ☐ Financial / Bank / Wire / Credit Card Fraud, Embezzlement, Theft Of Money, Money Laundering, Overtime Fraud, Contracting Fraud, Creating Fake Shell Companies To Bill Employer With Fake Invoices
- ☐ Employees Involved In Bribery, Kickbacks, Blackmail, Extortion
- ☐ Data, Computer & Network Sabotage / Misuse
- ☐ Employees Involved In Viewing / Distribution Of Child Pornography And Sexual Exploitation
- ☐ Employee Collusion With Other Employees, Employee Collusion With External Accomplices / Foreign Nations, Cyber Criminal - Insider Threat Collusion
- ☐ Trusted Business Partner Corruption / Fraud
- ☐ Workplace Violence(WPV) (Bullying, Sexual Harassment Transforms To WPV, Murder)
- ☐ Divided Loyalty Or Allegiance To U.S. / Terrorism

ORGANIZATIONS IMPACTED

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

- ☐ U.S. Government, State / City Governments
- ☐ Department of Defense, Intelligence Community Agencies, Defense Industrial Base Contractors
- ☐ Critical Infrastructure Providers
  - Public Water / Energy Providers / Dams
  - Transportation, Railways, Maritime, Airports, Aviation / Airline Industry (Pilots, Flight Attendants)
  - Health Care Industry, Medical Providers (Doctors, Nurses, Management), Hospitals, Senior Living Facilities, Pharmaceutical Industry
  - Banking / Financial Institutions
  - Food & Agriculture
  - Emergency Services
  - Manufacturing / Chemical / Communications
- ☐ Law Enforcement / Prisons
- ☐ Large / Small Businesses
- ☐ Defense Contractors
- ☐ Schools, Universities, Research Institutes
- ☐ Non-Profits Organizations, Churches, etc.
- ☐ Labor Unions (Union Presidents / Officials)
- ☐ And Others

INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

- ☐ Intellectual Property Theft (IP) / Trade Secrets Theft = Loss Of Revenue
- ☐ Embezzlement / Fraud (Loss Of $$$)
- ☐ Stock Price Reduction

Operational Impact / Ability Of The Business To Execute Its Mission

- ☐ IT / Network Sabotage, Data Destruction (Downtime)
- ☐ Loss Of Productivity
- ☐ Remediation Costs
- ☐ Increased Overhead

Reputation Impact

- ☐ Public Relations Expenditures
- ☐ Customer Relationship Loss
- ☐ Devaluation Of Trade Names
- ☐ Loss As A Leader In The Marketplace

Workplace Culture - Impact On Employees

- ☐ Increased Distrust
- ☐ Erosion Of Morale
- ☐ Additional Turnover
- ☐ Workplace Violence (Deaths) / Negatively Impacts The Morale Of Employees

Legal & Liability Impacts (External Costs)

- ☐ Compliance Fines
- ☐ Breach Notification Costs
- ☐ Increased Insurance Costs
- ☐ Attorney Fees
- ☐ Employees Loose Jobs / Company Goes Out Of Business

INSIDER THREAT INCIDENTS
FOR SEPTEMBER 2021

U.S. GOVERNMENT

7 Former U.S. Postal Service Employees Charged With Stealing Credit Cards From Mail - September 29, 2021

The indictments alleges that credit cards and other financial instruments were stolen from the mail and provided to others in exchange for cash or other items. Some of the defendants unlawfully obtained USPS customers' personal identifying information, including dates of birth and Social Security numbers, which was then used to fraudulently activate the stolen cards, the charges allege. The newly charged USPS employees delivered mail in Chicago or processed and sorted the mail at a USPS facility in suburban Palatine. (Source)

Former U.S. Postal Service Employee Admits To Stealing Credit Cards From Mail - September 23, 2021

From April 1 to July 23, 2019, Myriam Jimenez a postal service employee, admitted to stealing credit cards addressed to third-party victims and mailed to addresses on postal routes in Elizabeth and Roselle Park, New Jersey, that she provided to other individuals in exchange for offers of $100 per card. The fraudulent charges on the credit cards Jimenez stole totaled over $2,000. (Source)

Former U.S. Postal Service Employee Admits Stealing $35,000 Worth Of Cell Phones From Mail - September 16, 2021

Kyle Terry was employed by the U.S. Postal Service as a mail handle assistant at a national postal distribution center in Jersey City. From Nov. 1, 2017, to Jan. 28, 2018, Terry stole 39 cell phones having a total approximate value of $35,000 from mail that passed through that distribution center. (Source)

Former TSA Official Sentenced To Prison For Stealing $150,000 From Federal Worker's Compensation Program - September 9, 2021

Emmanuel Papas was injured on the job in 2004, when he served with the TSA at the Newark International Liberty Airport. apas began receiving federal worker's compensation benefits.

A subsequent federal investigation by TSA agents revealed that Emmanuel Papas was improperly receiving benefits because he was actively working at granite shops in the Myrtle Beach area from March 2009 through February 2020. Surveillance showed Papas working, interviews with various granite business employees confirmed that he worked at three Myrtle Beach-area retail granite shops, and deposits into Papas's bank account showed income from Myrtle Beach-area granite businesses. The investigation also revealed that Papas disguised his income by having his earnings either paid in cash or with checks made payable in his family members' names. Papas, who ultimately confessed, also completed at least eight federal forms attesting that he had no outside income and was, thus, eligible to continue to receive his benefits. The total loss to the federal government was just under $150,000. (Source)

Former Small Business Administration Employee Sentenced To Prison For Defrauding Ida Hurricane Victims & Using Funds For Personal Use - August 31, 2021

Keonna Davis was a disaster recovery specialist for the U.S. Small Business Administration. She pleaded guilty to wire fraud and aggravated identity theft.

Davis took personal information from people applying for disaster relief loans after Hurricane Harvey, obtained the loans and drew money from the applicants' accounts and used it to lease a $4,900 French bulldog and make other purchases totaling $285,430. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former NSA Subcontractor Employee Sentenced To Prison For Billing Government For 1,200 Hours Not Worked - September 2, 2021

According to her plea agreement, Company A was a subcontractor for Company B, providing employees that performed national security duties for the Department of Defense (DOD). From January 2017 until March 2019, Heyer worked for Company A, but was assigned on a day-to-day basis to work for the DOD on national security matters at the National Security Agency (NSA), in Fort Meade, Maryland.

From January 2017 through March 2019, Melissa Heyer used a badge reader to gain access to the SCIF. Heyer falsely represented to her employer that she had been working at the NSA SCIF when she was actually elsewhere. Heyer caused false claims to be submitted to the DOD that resulted in the government paying more than $100,000 for hours Heyer were not entitled to In total, as result Heyer knowingly caused the government to be billed for more than 1,200 hours of her time when she had actually not worked. (Source)

Active Duty Sailor And His Former Navy Colleague Are Charged With Conspiring To Traffic Guns - August 31, 2021

Elijah Boykin, an active-duty U.S. Navy Sailor, and Elijah Keashon Barnes have been indicted for unlawfully obtaining and transporting dozens of firearms that were later used in New Jersey-area crimes. Boykin and Barnes served together in the U.S. Navy until June 2020, when Barnes was discharged following his confinement for repeated violations of military law.

Between April 2020 and August 2020, Elijah Isaiah Boykin purchased more than two dozen firearms from federally licensed firearms dealers in Georgia and Virginia. The total purchase price exceeded $17,000 and was spread over eight transactions. On each occasion, Boykin signed paperwork stating that he was the actual purchaser of the guns but paid using a credit card belonging to co-defendant Elijah Keashon Barnes.

Local law enforcement in and around Newark, New Jersey began to recover Boykin's firearms shortly after they were purchased. One pistol was recovered in October 2020, when police officers in Newark conducted a traffic stop and arrested Barnes, who was wanted on a Virginia warrant for domestic assault and battery. The pistol was found in Barnes's car. A few months later, Newark police officers recovered another gun that Boykin purchased. Forensic testing linked that second firearm to three separate shootings in Newark, including a violent mugging during which a victim was shot multiple times in the right leg. (Source)

Navy Chief Warrant Officer Pleads Guilty To International Navy Bribery And Fraud Scandal - August 31, 2021

Retired Chief Warrant Officer Robert Gorsuch admitted in court he received more than $45,000 in bribes from foreign defense contractor Leonard Francis, who provided him with stays at luxurious hotels plus meals, entertainment and other gifts in exchange for official acts that would help Francis' ship husbanding business, including the disclosure of multiple classified ship schedules.

Gorsuch was one of 9 members of the U.S. Navy's Seventh Fleet indicted in March 2017 for participating in a conspiracy with Francis, the owner and CEO of Singapore-based Glenn Defense Marine Asia. (Source)

Marine Corps Colonel Pleads Guilty In International Navy Bribery & Fraud Scandal -September 3, 2021

U.S. Marine Corps Colonel Enrico DeGuzman pleaded guilty to a bribery charge today, admitting that he accepted more than $67,000 in extravagant meals, drinks, entertainment and hotel stays in Hong Kong, Singapore, and Tokyo from foreign defense contractor Leonard Glenn Francis.

DeGuzman admitted that in return for this and other things of value, he corruptly used his official position to assist Francis, the owner and CEO of Singapore-based Glenn Defense Marine Asia, a ship husbanding company that serviced U.S. Navy ships in the Asia Pacific region. DeGuzman admitted that he endeavored to influence Navy ships into ports serviced by GDMA; he shared confidential Navy information with Francis in order to help GDMA; and he helped with evaluating and indoctrinating potential new Navy members into Francis's cabal.

In one instance, DeGuzman joined Francis and others for a $40,000 meal that featured foie gras terrine, duck leg confit, ox-tail soup, and roasted Chilean sea bass, paired with expensive wine and champagne, followed by digestifs, cigars and overnights at the Shangri La - all at Francis's expense.

DeGuzman was one of nine members of the U.S. Navy's Seventh Fleet indicted by a federal grand jury in March 2017 for conspiring with Francis and for receiving bribes. DeGuzman is the second of the Seventh Fleet defendants to plead guilty. The trial of the remaining defendants was scheduled to begin November 1, 2021, but yesterday it was postponed until February 7, 2022. The remaining defendants - who are accused of trading military secrets and substantial influence for sex parties with prostitutes and luxurious dinners and travel - include U.S. Navy Rear Admiral Bruce Loveless; Captains David Newland, James Dolan, Donald Hornbeck and David Lausman; Commander Stephen Shedd; and Commander Mario Herrera.

The overarching fraud and bribery case has resulted in federal criminal charges against 34 U.S. Navy officials, defense contractors and the GDMA corporation. So far, 27 of those have pleaded guilty, admitting collectively that they accepted millions of dollars in luxury travel and accommodations, meals, or services of prostitutes, among many other things of value, from Francis in exchange for helping GDMA win and maintain contracts and over bill the Navy by over $35 million. (Source)

Former Veterans Administration Employee Pleads Guilty To Stealing Personal Protective Equipment & Other Medical Equipment For 11 Years, Then Selling For Personal Gain - September8, 2021

Chad Jacob pled guilty to stealing personal protective equipment (PPE), electronics, and medical equipment while working as the Assistant Chief of Supply Chain Management for the Gulf Coast Veterans Health Care System.

Beginning in 2009 and until December 2020, Jacob stole VA property which he resold at local pawn stores and on his personal eBay account. During the COVID-19 pandemic, Jacob stole N-95 masks and resold them for grossly inflated prices. In total, Jacob made more than $50,000 selling the stolen N-95 masks and over $9,000 selling stolen iPads and iPhones. (Source)

Former Veterans Affairs Employee Sentenced To Prison For Video Voyeurism Using Hidden Camera And Disorderly Conduct - September 24, 2021

Robert Sampson, while an employee of the Department of Veterans Affairs (VA), placed a hidden camera disguised to look like a cellular telephone charger power adapter, in a restroom at the Pensacola VA Joint Ambulatory Care Center. On approximately 17 occasions between May 2020 to June 2020, Sampson captured video of eight VA employees on the hidden camera. When employees discovered the recording device and notified the VA Police, Sampson attempted to wrestle the employees for control of the device. Sampson later admitted that he had placed the device in the restroom to record individuals in the bathroom and would later watch the footage. (Source)

Former Air Force Employee Pleads Guilty To Receiving Stolen Government Money ($55,000) Through Falsified Travel Claims - September 28, 2021

Anthony Jones had been employed with the Department of the Air Force. During his employment, Jones sustained injuries and applied for and received worker's compensation money under the Federal Employees' Compensation Act. As part of his compensation, Jones was able to be reimbursed for travel expenses to and from medical appointments related to his injuries. From May 4, 2016, through August 22, 2019, Jones filed hundreds of false travel claims for medical appointments and was reimbursed approximately $55,210.50 resulting from those false travel claims. At his plea hearing, Jones admitted that he intended to keep the money and that he knew the money was stolen. (Source)

Former Walter Reed (WR) Medical Center Department Head Sentenced To Federal Prison for Accepting Cash, Event Tickets & Other Gratuities From Company That Received More Than $25 Million In Government Business From WR - September 30, 2021

From 2009 until May 2019, David Laufer worked as the Chief of the Prosthetics at the Department at the WR National Military Medical Center.

Bruce Thomas owned, operated, and controlled Pinnacle Orthopedic Services Pinnacle provided prosthetics and related materials to Walter Reed in return for payments from the government.

Between 2012 and 2016, Laufer and his wife received things of value, such as airlines travel, lodging and entertainment tickets, as well as direct cash payments from Pinnacle. Laufer admitted that he undertook official acts in connection with the gratuities, including seeking renewal of Blanket Purchase Agreements (BPA's) with Pinnacle, sending multiple purchase requests obligating millions of dollars to Pinnacle for prosthetics and related materials, causing the BPA's repeated ordering of supplies from Pinnacle. (Source)

LAW ENFORCEMENT / FIRST RESPONDERS / PRISONS

Former Police Officer Pleads Guilty To Illegally Obtaining $60,000 Payment For Hours He Did Not Work - September 29, 2021

Ricky Perry, formerly a police officer with the Village of Alorton Police Department, entered a plea of guilty to Obtaining Funds by Fraud from the Village of Alorton Police Department, a Unit of a Government that Received Federal Funds.

Perry acknowledged that he obtained funds by fraud from May 2018 through April 2021 claiming to be working when he was out of the jurisdiction, usually at his residence in East St. Louis. The Information alleges that there was approximately 4000 hours where Perry claimed he was working but he was outside the jurisdiction of the Village of Alorton causing a financial loss of approximately $60,000. (Source)

Former Correctional Officer Pleads Guilty To Attempting To Smuggle Drugs Into Prison For Bribe - September 8, 2021

Leslie Spencer worked as a correctional officer in Fort Myers at the Charlotte Correctional Institution's offsite work camp. In March 2021, Spencer agreed to smuggle three ounces of methamphetamine, one ounce of MDMA, a small amount of synthetic marijuana, and two cell phones into the prison and provide it to an inmate in exchange for a payment of $400. (Source)

Former Treasurer For Fire Department Union Charged With Embezzling $220,000+ Of Union Funds For Luxury Lifestyle - September 27, 2021

Verdine Day was the Treasurer of the Detroit Fire Department Union (DFFA) from 2015 to 2019.

Day fraudulently obtained approximately $167,900.00 of union funds by (1) issuing checks in her name and then changing the name of the payee in the Union's QuickBooks software (2) cashing checks which were voided by her in QuickBooks and (3) writing checks made payable to cash.

Day also used DFFA credit cards as her own personal credit cards while she was Treasurer and after she retired. In total, she charged approximately $52,143.65 in personal expenses using DFFA credit cards. Her purchases on DFFA credit cards included flights, hotel rooms, cruises, car insurance premiums, satellite and cable TV service, national and state parks fees, and furniture. Day used a DFFA union credit card to charge $9,553 for a cruise with Royal Caribbean cruise lines in 2017. Day also used a union credit card to pay for another Royal Caribbean cruise costing $8,975 on the Liberty of the Seas in 2019. She used the union's credit card to pay her bar bill at a casino in Ohio in May 2019 and for a meal at a Bubba Gump Shrimp Co. restaurant in Cozumel, Mexico in 2019. (Source)

Former Prison Cook Sentenced To Prison For Methamphetamine Trafficking And Bribery - August 30, 2021

Hank Williams is a former Cook Supervisor at United States Penitentiary Big Sandy.

Williams admitted to conspiring with an inmate and others to distribute 50 grams or more of methamphetamine. Williams, a public official, also accepted bribes from the inmate and others, and used the U.S. mail to possess and distribute the controlled substances. (Source)

STATE / CITY GOVERNMENTS / SCHOOL SYSTEMS

Former New York State Employee Pleads Guilty To $300,000+ Unemployment Insurance Fraud - September 21, 2021

Tramaine Pope admitted to abusing her position as a New York State Department of Labor (NYSDOL) employee to obtain $314,168 by submitting and approving 20 false unemployment insurance applications. The funds stolen by Pope included benefits from federal programs intended to help out-of-work New Yorkers during the COVID-19 pandemic.

Pope admitted to receiving lists of names and personal identifying information from another individual. Pope then used her access to NYSDOL systems to submit and approve fraudulent unemployment insurance claims using the names and other information she received. (Source)

Former Massachusetts State Representative Sentenced To Prison For Embezzling $33,000+ Of Campaign Funds For Personal Use (Bought Home, Paid Debts) - September 15, 2021

Former Massachusetts State Representative David Nangle was sentenced to prison for illegally using campaign funds to pay for his personal expenses, defrauding a bank to obtain loans to purchase his home and repay his personal debts, and collecting income that he failed to report to the Internal Revenue Service.

During the period of the charged offenses, Nangle was heavily in debt and gambled extensively at area casinos and online, and then used thousands of dollars in campaign funds to pay for various personal expenses such as dues at a local golf club, rental cars to travel to casinos, flowers for his girlfriend, gas, hotels and restaurants. Nangle concealed his theft by filing false reports that disguised the personal nature of the spending.

Upon learning of the investigation into his embezzlement and fraud, Nangle also obstructed justice by entering into a sham consulting agreement with a local business owner designed to make payments he received appear legitimate. In reality, Nangle never provided any legitimate services in exchange for receiving $27,000 from that business owner. Instead, Nangle helped the business owner curry favor with an important client by sponsoring legislation that benefited the business owner's client. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

Former Church Employee Sentenced To Prison For Stealing $270,000+ From Church Over 4 Years To Pay Credit Card Bills- September 24, 2021

Melissa Noland was employed by a church between January 2015 and January 2019. During that time, Noland stole money from the church in various ways. Noland wrote checks to herself using the church's checkbook, used church bank accounts to pay her own credit card bills, and made excess payroll distributions to herself. Noland eventually stole $274,222.09 from the church. Once the church discovered her thefts, she was terminated from her employment. (Source)

Former Chief Financial Officer Pleads Guilty To Embezzling From Religious Charity For Personal Use - September 8, 2021

In March 2012 Lynch became the CFO of the Holy Cross organization, and in January 2015 he became its CEO.

Lynch admitted that when he was Holy Cross's CEO, he used Holy Cross funds to pay for repairs to his own cars, install a new roof on his house, pay down his personal mortgage balance, and make payments on a personal American Express account. Lynch also used Holy Cross funds to pay his own consulting company and to pay another company hired to provide security services at the Samaritan Center, a company ostensibly controlled by a relative but actually controlled by him.

Lynch attempted to justify some of these payments with bogus invoices. In addition, Lynch used his corporate Holy Cross American Express card to pay for goods and services of a personal nature. (Source)

Ex-Chairman Of Church Sentenced To Prison For Stealing $11 Million+ Of Church Funds To Buy Home - August 30.021

The church hired Charles Sebesta in 2001 as its facilities manager. He joined the church four years later and ultimately served as its chairman, giving him control over the church branch's financial assets and operations, including some of its bank accounts.

From August 2006 through December 2016, Sebesta caused the church to make checks and other payments to banks accounts in the name of fictitious companies he created, as well as to bank accounts he held in his own name and in the names of his family members and a female companion. To conceal these payments, Sebesta forged a church member's signature on numerous checks drawn against the church's bank accounts.

In the fall of 2008, Sebesta oversaw the sale of church property for approximately $12.8 million. Sebesta stole a significant majority of the proceeds for his personal use, including purchasing a home with more than $2 million in cashier's checks drawn from church bank accounts.

In 2009 and 2010, Sebesta used church money to wire $1.86 million and $309,622 to be credited to his own personal tax accounts to generate overpayment refunds from the U.S. Treasury and the California Franchise Tax Board.

To conceal his crimes, Sebesta impersonated a real estate developer by creating an email account in the executive's name. Posing as the developer, Sebesta sent emails to church members in which he fraudulently represented that the real estate developer held Sebesta in high esteem and was making donations to the church and paying the rent for the church's new location.

Sebesta also defrauded another former employer, a private high school, out of $34,032 and embezzled $36,282 that a donor's estate had donated to the church. (Source)

Former Religious Organization Employee Sentenced To Prison For Taking $229.000+ In Kickbacks And Using For Personal Use - September 2, 2021

February 2008 until July 2019, Charles David was employed as the Director of Building and Construction by a Jacksonville-area religious organization. David's role and responsibilities included overseeing sales of land belonging to the religious organization. He understood that it would be a conflict of interest for him to receive compensation from a third-party in connection with these land sales.

Beginning in 2013, David engaged in a scheme to defraud the religious organization by offering the organization's land for sale exclusively to two individuals, excluding other potential purchasers. In exchange for giving that preference to those individuals, they paid David kickbacks totaling $229,500. After the two individuals purchased the land, they resold it at a significant profit. David admitted that he sold the religious organization's land for at least $229,500 less than it was worth. David did not disclose the kickbacks to the religious organization and used at least $72,000 of the kickbacks to fund mortgage payments and settlement costs associated with real property owned by his wife. (Source)

PHARMACEUTICAL COMPANINES / PHARMICIES / HOSPITALS / HEALTHCARE CENTERS / DOCTORS OFFICE

2 Hospital Nurses Held Accountable For Taking Controlled Substances From Patients For Personal Use - August 30, 2021

Katie Muhs was employed as a registered nurse in the Intensive Care Unit at a hospital in Colorado in 2019 when she used her position to divert fentanyl, a schedule II controlled substance, for her own personal use. The defendant admitted that between June 2019 and September 2019, she stole fentanyl by removing it from the IV bags of ventilated patients using a sterile syringe.

Alicia Tangeman used her position as Registered Nurse to access the rooms of patients she was not assigned to care for in a separate unit of a Colorado hospital. She falsely and fraudulently told patients that she was conducting a "study" on the effectiveness of Patient-Controlled Analgesia (PCA) pumps, which deliver controlled substances to hospital patients to relieve pain on-demand when the patient pushes a button. She then used a key to open the machine that secured the syringe of hydromorphone that was to be dispensed to the patient. She removed a portion of the drug from the syringe, which she kept, then returned the syringe to the patient's PCA. She illegally obtained controlled substances in this way from three patients on four occasions. When confronted by law enforcement regarding her actions, the defendant lied about the diversions and persisted in her false story that she was engaged in a study with a well-known university. The defendant engaged in obstructionist conduct by producing to law enforcement a false e-mail that she stated came from a friend who asked her to participate in the research. The defendant created the false e-mail herself using a fictitious e-mail account she created in the name of this alleged friend. (Source)

Former Nurse Assistant Working For Rehabilitation Facilities Accused Of Stealing Patients Banking Information To Lease Apartments / Purchase Vehicles - September 17, 2021

Sierra Johnson worked at various rehabilitation facilities where 7 patients had reported the theft of their banking information and social security numbers.

The stolen information was used to make expensive purchases, including $19,000 for a brand new car and $2,600 for multiple wigs.

To buy the vehicle, a creditor asked for a photograph of the purchaser. Tempe police said the photo received appeared to be a picture of Johnson that had been manipulated to make her look older.

Some patients had their identities used to sign lease agreements on rentals costing $1,700 in monthly rent or to buy up to $950 in new furniture.

Police said Johnson's boyfriend may have been involved in the fraudulent schemes. (Source)

Former Nurse Sentenced To Prison For Drug & Health Care Fraud Charges - September 20, 2021

According to court documents, Joseph Mattingly diverted Schedule II controlled substance (Hydrocodone) pills from a patient and defrauded the Medicare program of the cost of the pills.

In 2018, Mattingly was employed as a nurse with Progress Port, a center for adults with intellectual disabilities in Williamson County. Between August 20, 2018 and October 30, 2018, Mattingly obtained possession of 25 Hydrocodone pills he falsely claimed he dispended to a Progress Port resident, which he diverted for his own personal use.

Mattingly took three Hydrocodone pills intended for the same Progress Port resident and replaced those pills with Tylenol, an over-the-counter medication at three separate locations. (Source)

Former Emergency Medical Services Worker Sentenced To Prison For Stealing With Fentanyl & Hydromorphone - September 16, 2021

Jeffery Leedy tampered with at least 50 vials of fentanyl and hydromorphone while working at Centra Lynchburg General Hospital and as an Emergency Medical Services (EMS) worker for Roanoke County Emergency Medical Services.

On May 16, 2019, a Roanoke City EMS ambulance crew member discovered a suspected tampered vial of fentanyl while on an EMS call. When he attempted to administer the vial to a patient, he noticed the vial's cap was not secured and believed the vial had been tampered with. Further investigation revealed that Leedy had tampered with the vial by removing the fentanyl and replacing it with saline.

A supervisor with the Roanoke County EMS queried the access card database and determined that Leedy had been accessing the rescue squad building at night, while he was not working, to take fentanyl. Further investigation revealed at least 50 vials of fentanyl and hydromorphone had been tampered with. (Source)

Former Hospital Employee And Accomplice Sentenced To Prison For $825,000+ Hospital Fraud Scheme - September 10, 2021

Aaron Hill worked as a Human Resource Coordinator at Community Health Services in Franklin, Tenn. where he was responsible for selecting recruiting vendors on behalf of his company.

Around August 2015, Hill and Tyrone Berry agreed to create false invoices for "Berry Recruiting," a company purportedly owned by Berry. Berry scoured various social media websites and pages such as LinkedIn and Craig's List to obtain the names of unsuspecting job seekers. Hill submitted invoices to Community Health Services for payment, representing that these persons were recruited Berry Recruiting. Berry Recruiting received $257,469.84 for 38 false invoices submitted to Community Health Services between August 2015 and April 2016.

Hill and Berry carried out a similar scheme at Quorum Health Corporation in Brentwood, where Hill began working in May 2016 as an Employee Relations Manager. Hill and Berry subsequently submitted false invoices to Quorum Health on behalf of Berry Recruiting. Berry Recruiting received $567,765 for 33 false invoices, all of which falsely represented Berry Recruiting obtained and relocated new employees. The investigation determined Hill and Berry simply recycled the names of employees previously recruited by other firms and hired by Quorum Health.

Between August 2015 through April 2017, Hill and Berry obtained over $825,000 from the two companies, and thereafter split the unlawful proceeds. (Source)

Former Doctor For Medical Practice Admits To Stealing $500,000+ From Employer Over 5 Years To Pay Personal Expenses - September 9, 2021

Dr. Walter Sytnik admitted defrauding his prior employer's medical practice by stealing and forging the medical practice's checks to pay personal expenses/

Before attending medical school, Sytnik worked for a medical practice in southern New Jersey as a bookkeeper. While employed by the practice, Sytnik stole some of its checks and, from May 2013 through April 2018, used them to steal more than $500,000 from the practice. He opened and maintained credit card accounts at the same banks as used by the doctor at the medical practice, and forged the doctor's signature on the stolen checks, which he sent through the U.S. Mail to pay his own credit card bills. When Sytnik ran out of checks, he reordered new ones so that he could continue the fraud. (Source)

TRADE SECRET THEFT

Former Engineer Pleads Guilty During Trail Of Conspiring To Steal Trade Secrets With Help Of Co-Conspirators - September 29, 2021

Gilbert Basaldua worked as a numerical control engineer contractor for an aircraft manufacturer in the Southern District from October 2016 through November 2018. During that time, Basaldua conspired with his co-conspirators to steal valuable proprietary aircraft wing designs and anti-icing testing information from various aircraft manufacturers, including the company where Basaldua worked. The conspirators intended to use the stolen information to quicken the process of obtaining Federal Aviation Administration certification for another company's product. (Source)

BANKING / FINANCIAL INSTITUTIONS

Former Credit Union Employee Pleads Guilty To Unauthorized Access To Computer System After Termination & Sabotage Of 20+GB's Of Data - August 31, 2021

Juliana Barile was fired from her position as a part-time employee with a New York Credit Union on May 19, 2021.

Two days later, on May 21, 2021, Barile remotely accessed the Credit Union's file server and deleted more than 20,000 files and almost 3,500 directories, totaling approximately 21.3 gigabytes of data. The deleted data included files related to mortgage loan applications and the Credit Union's anti-ransomware protection software. Barile also opened confidential files. After she accessed the computer server without authorization and destroyed files, Barile sent text messages to a friend explaining that "I deleted their shared network documents," referring to the Credit Union's share drive. To date, the Credit Union has spent approximately $10,000 in repairing the damages of the unauthorized intrusion and destruction of data. (Source)

Former Bank Teller Charged With Embezzling $63,000+ - September 10, 2021

Between November 2017 and February 2020, Demetria Silvio held the positions of head teller, universal banker, and mortgage loan assistant at Iberia Bank in New Orleans and Metairie.

From December 3, 2018 to December 6, 2019, Silvio embezzled approximately $63,059.82 from five customer accounts by forging approximately 66 counter checks. Silvio deposited the fraudulent checks into her own bank accounts with Chase Bank and Capital One. (Source)

Former Bank Employee Charged In 2 Fraud Schemes - September 16, 2021

Between approximately June 2014 and November 2018, Rushell Harris engaged in two separate wire fraud conspiracies.

In the first conspiracy, Harris allegedly exploited her position at Nantucket Bank by obtaining personal identifiable information of a customer and surreptitiously taking photographs of the victim's account information. It is alleged that Harris then shared that information with co-conspirators who attempted to transfer funds out of the customer's bank account without authorization.

In the second conspiracy, Harris allegedly helped perpetuate a fraudulent lottery scheme targeting at least 13 victims. Victims were contacted by co-conspirators via phone and were informed they won large prizes, and that in order to receive the funds they needed to pre-pay taxes on their winnings. In reality, no such prizes existed. After victims made an initial payment, they were advised that additional advance payments were required for expenses such as insurance, transportation or other international customs' fees. It is alleged that Harris and her co-conspirators transferred proceeds of the scheme to associates in Jamaica and in the United States. (Source)

Former Bank Manager Sentenced To Prison For $10 Million+ Money Laundering Scheme - September 3, 2021

Between February 2017 and August 2019, Carlos Vasquez, while branch manager at a bank in Rio Rico, Arizona conspired to launder money for a group of individuals to conceal the illegal source of the funds. As part of this conspiracy, the money laundering organization brought Mexican citizens into the bank and Vasquez set up accounts for them for the purpose of sending illegal funds back to Mexico. Once the bank accounts were established, the money laundering organization openly handed cash to the Mexican citizens for deposit into the funnel accounts. The Mexican citizens then wired the funds into Mexican bank accounts under the direction of the money laundering organization.

Vasquez admitted that these funnel bank accounts enabled Vasquez and his branch to appear to have attracted new customers for the bank, improving the bank's sales performance. Vasquez also admitted to knowing that the head of the money laundering organization was a former customer of the bank and that the funds moving through the accounts were proceeds of unlawful conduct. Vasquez personally authorized 42 wire transfers out of the funnel accounts to bank accounts in Mexico in the amount of $357,883. Over the course of the conspiracy, the money laundering organization allegedly moved over 10 million dollars in drug proceeds through the bank. (Source)

EMBEZZLEMENT / FINANCIAL THEFT / BRIBERY / KICKBACKS / EXTORTION / MONEY LAUNDERING

Former Executive Director Of The Economic Development Authority For Front Royal Virginia Charged With Bank Fraud / Money Laundering For Personal Use - August 31, 2021

Jennifer McDonald was the Executive Director of the Economic Development Authority (EDA) from April 2008 until December 2018. From June 3, 2014 to December 20, 2018, McDonald devised and participated in a scheme to defraud the EDA to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises.

McDonald had access to funds belonging to the EDA and used the funds to pay on debt owed by her, other individuals, and LLCs she controlled, to purchase real property for which she often earned commissions as a real estate agent, and to purchase real property in the name of an LLC she controlled. (Source)

Former Office Manager Sentenced To Prison For Embezzling $600,000 From Employer - September 27, 2021

From 2014 to 2018, Joan Chenoweth, who had control of the business's financial records as well as control of and access to the business's credit cards and bank account, wrote unauthorized vendor checks to herself or to cash payable from her employers bank account; wrote unauthorized payroll checks to herself that exceeded her salary; and used the business's credit cards to make payments to her personal credit cards. She used her position as office manager to avoid detection by making false entries in the business's financial records. (Source)

Terminated Employee Charged With Sending Threats To Employer With Intent To Extort Money From Employer And Coworkers - September 23, 2021

According to the indictment brought on Aug. 12, 2021, William Robinson worked at a business from June to November in 2017. After the business fired him, Robinson began sending threatening messages to his former supervisor and other coworkers in an attempt to extort them for money. These threats included graphic statements threatening to physically harm the supervisor's daughter. Robinson made the threats because he wanted the company to pay him between $10,000 and $20,000. (Source)

Former Financial Services Representative Convicted Of $570,000 Fraud Scheme To Pay For Personal Expenses - September 23, 2021

From 2004 to 2016, Sampson Pearson was a representative for a financial services firm. Pearson offered and sold life insurance products and annuities as an independent contractor for a company.

Pearson used his position to defraud at least 10 victims and a company of more than $570,000 through a fraudulent loan and disbursement scheme. Pearson executed the scheme by submitting falsified loan applications and requests for disbursements in the victims' names without their knowledge and approval. The company authorized the loans and disbursements based on the fraudulent documents submitted by Pearson. Pearson also directed the company to deposit the fraudulently-obtained funds into an account he controlled. Pearson used the funds to pay for personal expenses and to fund his lifestyle. (Source)

Former Trucking Company Manager Sentenced To Prison For Defrauding Company Of More Than $600,000 - September 23, 2021

Timothy Mayer was the manager of Jung Truck's.

Mayer admitted that beginning in July 2019, he started charging expensive tires to Jung Truck's accounts at a local tire supplier. Mayer then sold the tires on the side and pocketed the cash. The value of the tires that Mayer fraudulently charged to Jung Truck exceeded $590,000. Mayer also stole tires and brakes from Jung Truck's inventory and sold those items on the side. In total, Mayer caused Jung Truck to sustain a loss of more than $620,000. The scheme lasted until Mayer was caught in May 2020. (Source)

Former Office Manager Pleads Guilty To Embezzling $233,000+ From Employer - September 23, 2021

Aurelia Stanton worked as an office manager from approximately June 2014 through May 2017 for a business. She was responsible for ensuring timely payment of bills and invoices, accurate bookkeeping, and managing the office. From August 2015 through May 2017she embezzled more than $233,000 writing checks to herself on the company's check stock. She used a computer software program to conceal the fraudulent disbursements by editing the company's bank statements to remove references to the fraudulently drafted, forged, and negotiated checks. In total, she deposited 187 checks with forged signatures. (Source)

Former Chick-fil-A Employees Pleads Guilty To Stealing $492,000 To Support Luxury Lifestyle - September 21, 2021

Larry Black is the former Director of Hospitality at Chick-fil-A Five Points. He pleaded guilty to conspiracy to commit wire fraud and bank fraud before U.S. District Judge Madeline H.

Black's co-defendant, Joshua Powell a former manager at the same location, pleaded guilty to conspiracy to commit wire fraud in June.

Between April 2018 and January 2018, Black and Powell devised and implemented a scheme to divert $492,000 in customer payments to bank accounts under their control. Black and Powell used these accounts to receive customer credit card payments intended for Chick-fil-A Five Points. Many of these payments were for catering orders from large customers. To effectuate the scheme, Black and Powell used fraudulent email and digital payment accounts that imitated the look of official Chick-fil-A accounts. In addition to these fraudulent "Chick-fil-A" accounts, Black and Powell also utilized a personal email account belonging to Powell to intercept virtual credit card payments that were made on behalf of an additional customer. Black used the fraud proceeds to support his lifestyle, including the purchase of high-end luxury vehicles and vacations. (Source)

Former Union Treasures Sentenced To Prison For Embezzling $184,000 From Union For Personal Expenditures - September 21, 2021

From in or about January 2016 through in or about April of 2020, Yvette Luster was an employee of Postal Mail Handlers Local 314 labor union, acting as the local chapter's Treasurer. In her capacity as Treasurer, Luster had access to Local 314's bank account.

Luster made over 200 unauthorized withdrawals from the union's bank account for personal expenditures, such as flights and meals for herself and family members unrelated to the business and operations of Local 314. In total, Luster embezzled over $184,000.00 from the union. (Source)

Former Manager For Guided Tour Company Admits To Embezzling From Employer With Help Of Another Employee - September 20, 2021

Between October 2010 and August 2016, Estela Laluf held a management position at a New Jersey guided-tour company.

During that time, Laluf and another employee, who held an accounting position at the company and had authority to write checks against the company's bank accounts, devised a scheme to embezzle funds from the company. Laluf would direct the employee to write company checks to actual company employees and contractors, which did not reflect any actual work or services done by those individuals. The employee would then cash these checks, and Laluf and the employee would convert the resulting funds to their personal use. Laluf and the employee embezzled hundreds of thousands of dollars from the company. (Source)

Former Sales Manager Sentenced To Prison For $738,000+ Of Wire Fraud Scheme Over 8 Years For Personal Use - September 18, 2021

This wire fraud scheme began around January 2010 and continued through September 2018. Dallas Harkness was a sales manager for Curry Seed Company located in Elk Point, South Dakota. On multiple occasions during the course of the scheme, Harkness received checks from Curry Seed customers as payment or pre-payment for seed. Instead of sending the checks to Curry Seed for deposit, Harkness falsely and fraudulently deposited some of those customer checks into checking accounts he controlled. Harkness then used the funds for his purposes. (Source)

Former Procurement Manager Sentenced To Prison For Embezzling $397,000+ From Employer - September 17, 2021

From September 2012 until February 2019, Marwan Kawar devised a scheme to defraud his employer by creating, approving, and submitting payment for fraudulent purchase orders, invoices and shipping receipts in the name of a sham company that he created and controlled. These invoices caused his employer to mail checks to his sham company for goods and services they never received.

Kawar attempted to flee the country before his sentencing, but federal agents apprehended him at the O'Hare Airport before he could board the flight. The cash he had in his possession at that time will go towards his restitution owed to the victim. (Source)

Former Accounting Coordinator For Non-Profit Organization Sentenced To Prison For Embezzling $321,000+ - September 16, 2021

Danielle Strother-Rush was an Accounting Coordinator for the Eastern Minority Supplier Development Council, which is a nonprofit organization that was created to increase business opportunities for minority-owned businesses.

From approximately August 2014 until August 2016, Strother-Rush embezzled $321,255.88 in various ways. The primary way in which she embezzled funds was by writing checks to herself from the operating accounts and forging her supervisor's signature on the checks. She also made unauthorized ATM withdrawals including several at the Rivers Casino. Lastly, she accessed the payroll bank account online and made unauthorized electronic checks payable to herself. (Source)

Former Chief Financial Officer Sentenced To Prison For $30 Million Embezzlement Scheme For Personal Use - September 15, 2021

The former Chief Financial Officer of Alden Shoe Co. was sentenced today for embezzling approximately $30 million from the company as part of a long-running scheme.

Richard Hajjar, 64, of Duxbury, was sentenced by U.S. District Court Judge Nathaniel M. Gorton to 70 months in prison and three years of supervised release. Hajjar was also ordered to pay restitution of $33,962,880 and forfeiture of $27,300,552. On May 5, 2021, Hajjar pleaded guilty to one count each of wire fraud, unlawful monetary transactions and filing a false tax return.

From at least 2011 through October 2019, when Richard Hajjare was terminated by Alden Shoe Co., Hajjar embezzled money by writing checks to himself from company bank accounts and transferring funds from company accounts to his personal accounts and to another individual. In total, Hajjar embezzled approximately $30 million which he used to enrich himself and to buy gifts and luxury travel for others close to him, including private flights to the Caribbean and diamond jewelry. (Source)

Former Treasurer / Comptroller Sentenced To Prison For $1.5 Million+ Of Bank Fraud - September 15, 2021

Sophia Kim, was the former Treasurer and Comptroller for the Universal Ballet Foundation, which operated the Kirov Academy of Ballet, a non-profit organization located in the District of Columbia.

Between approximately January 2018 and September 2018, Kim misappropriated approximately $1.5 million from the organization's bank accounts through unauthorized check, debit, and credit card transactions.

This consisted of 68 unauthorized checks to "Cash" or to "Sophia Kim," in whole-dollar amounts ranging from $500 to $12,000, totaling approximately $377,200, 197 unauthorized debits and cash withdrawals, totaling approximately $479,283, and 139 unauthorized credit card transactions, totaling approximately $681,751. More than $1 million of unauthorized debits and withdrawals and credit card charges were at MGM National Harbor Casino in Oxon Hill, MD, totaling approximately $1,068,026.

At the time that Kim began committing these offenses, she had just completed a period of supervised release for an earlier conviction stemming from her work as a bookkeeper and treasurer of another non-profit. In that case, she was convicted in 2012 in the U.S. District Court for the Eastern District of Virginia on charges of filing a false tax return and tax evasion and sentenced to two years in prison, to be followed by three years of supervised release. (Source)

Former Amazon Employee Pleads Guilty To Involvement In Amazon $100 Million Marketplace Fraud Ring - September 8, 2021

Rohit Kadimisetty, who after leaving Amazon in 2015 launched a consulting firm for third-party sellers, admitted that he conspired to commit bribery across state and national borders.

Kadimisetty said he bribed former Amazon colleagues in exchange for confidential information about sellers on the platform. The information gave Kadimisetty's clients an unfair competitive advantage on the Amazon Marketplace.

Kadimisetty also admitted to paying Amazon employees to disable other sellers' product listings to route shoppers to the listings of Kadimisetty's clients. And he acted as a go-between to help other Marketplace consultants, some of whom were indicted as his co-defendants, to arrange similar services on behalf of their clients.

The U.S. Attorney estimated last year that the monetary toll of the fraud ring was in excess of $100 million, a sum that includes the proceeds of merchants who benefited from the conspiracy, lost sales on the part of their competitors and costs to Amazon. (Source)

Former Employee For Nonprofit Organization Pleads Guilty To Theft Of $4.7 Million Of Federal Funds Over 7 Years For Personal Use - September 13, 2021

Ruth Phillips worked at River Valley Child Development Services (RVCDS) from December 1986 until September 2020. Phillips held various positions at RVCDS, including Director of Business and Finance. Phillips was responsible for all financial operations, including monitoring accounts receivable, creating and submitting invoices, reconciling bank accounts and issuing checks.

From July 2016 to June 2017, RVCDS received approximately $7,131,756 in federal funding and Phillips used her position of trust and authority to steal approximately $964,012 during that period.

Phillips further admitted that between December 2013 and August 2020, she stole approximately $4,721,731 from RVCDS. During that period, she sent $1,142,500 to her personal checking account and sent another $3,395,500 to Attitude Aviation's U.S. bank account. Attitude Aviation has offices at Lawrence County Airpark in South Point, Ohio, and Tri-State Airport in Huntington and provides aeronautical services, including fueling, rental of hangar space, aircraft rental, flight instruction and maintenance. (Source)

Former Employee Charged With $300,000 Wire Fraud And Identity Theft Scheme Against Employer Over 6 Years - September 10, 2021

From March 27, 2014 and continuing through at least September 29, 2020, Ronald Miller devised a scheme to defraud his employer out of at least $300,000. The investigation revealed Miller fraudulently drafted and submitted false weekly timesheets reflecting work that employees did not perform. The indictment further alleges that it was part of the defendant's scheme to defraud that he submitted fraudulent invoices and altered receipts so that his employer would pay him money that he was not entitled to receive. (Source)

Packaging Company Controller Sentenced To Prison For Stealing Funds Forcing Company Out Of Business - September 7, 2021

Victoria Mazur was employed as the Controller for Gateway Packaging Corporation, which was located in Export, PA. From December 2012 until December 2017, she issued herself and her husband a total of approximately 189 fraudulent credit card refunds, totaling $195,063.80, through the company's point of sale terminal. Her thefts were so extensive, they caused the failure of the company, which is now out of business. In order to conceal her fraud, Mazur supplied the owners with false financial statements that understated the company's true sales figures. (Source)

UNIVERSITIES / EDUCATION / SCHOOLS

Former Office Manager For Boys School Sentenced To Prison For $240,000 Wire Fraud Scheme - August 31, 2021

Katherine Torres was employed as an office manager for Pine Haven Boys School in Allenstown, New Hampshire from 2012 until March 25, 2019. Torres was the sole employee responsible for administering payroll. On various occasions, Torres submitted false information to Pine Haven's payroll company, causing direct deposits to be made into her personal bank accounts. In total, Torres received approximately $240,000 through this scheme. (Source)

Yale University School Of Medicine Employee Charged With Stealing & Selling Millions Of Dollars In Computer Hardware - September 3, 2021

Beginning in approximately 2008, Jamie Codrington was employed by the Yale University School of Medicine (Yale Med), Department of Emergency Medicine, and most recently served as the Director of Finance and Administration for the Department of Emergency Medicine. As part of her job responsibilities, Petrone-Codrington had authority to make and authorize certain purchases for departmental needs as long as the purchase amount stayed below $10,000. Beginning at least as early as 2013, Codrington engaged in a scheme whereby she ordered, or caused others working for her, to order millions of dollars of computer hardware from Yale vendors using Yale Med funds and arranged to ship the stolen hardware to an out-of-state business in exchange for money.

It is further alleged that Codrington falsely represented on Yale internal forms and in electronic communications that the hardware was for specified Yale Med needs, such as particular medical studies, and she broke up the fraudulent purchases into orders below the $10,000 threshold that would require additional approval. The out-of-state business, which resold the computer hardware to customers, paid Petrone-Codrington by wiring funds into an account of a company in which she is a principal. (Source)

DATA / COMPUTER / NETWORK MISUSE & SABOTAGE

Information Technology Assistant Manager Accused Of Crypto-Mining Using Employers Network - September 14, 2021

An information technology expert employed by a New York county has been arrested on suspicion of mining crypto-currency at work.

Christopher Naples is accused of covertly installing dozens of machines throughout his workplace and using them to mine Bitcoin and other types of crypto-currency as part of a secret illegal money-making scheme.

Naples was hired by Suffolk County back in 2000. His current title is Assistant Manager of Information Technology Operations for the Suffolk County Clerk's Office.

Authorities said that the clandestine crypto-mining activity allegedly carried out by 42-year-old Naples ran up electricity bills in excess of $6,000 for his unsuspecting employer. The mining devices increased the temperature in some rooms by 20 degrees.

Naples is accused of installing 46 crypto-mining devices in six rooms inside the county center located in Riverhead, New York. Hiding places in which the devices were allegedly concealed included beneath the floorboards of the building, on top of or inside server racks and inside an electrical wall panel that was not in use. (Source)

AT&T Employees Received More Than $1 Million In Bribes To Install Malware / Key Logger On Company's Network - Costing AT&T $201 Million+ - September 16, 2021

Muhammad Fahd, a citizen of Pakistan and Grenada, paid more than $1 million in bribes to AT&T employees in the summer of 2012, to install malware on the company's internal network. He has been sentenced to 12 years in prison after he illegally unlocked more than 1.9 million phones, causing the AT&T losses in excess of $201 million.

Using Facebook as a means to communicate, Fahd promised large payments of money if call center employees agreed to unlock phones so they could be sold and used outside AT&T's network. To receive their bribes, Fahd told AT&T employees to create shell companies and open business banking accounts in the names of the shell companies. Fahd recuperated the bribes by selling phone unlocking services through the now-defunct SwiftUnlocks.com website.

The scheme lasted only for a few months, until April 2013, when AT&T implemented a new phone unlocking procedure and call center employees Fahd had bribed either left or were fired by AT&T. Seeking to go around AT&T's new unlock system Fahd then bribed another employee to install the malware / key logger inside AT&T's call center to collect information from inside the network, including network layout and employee credentials. A second version was more sophisticated and deployed at a later stage, acting as a remote access tool and allowing Fahd easy access to AT&T's internal applications. (Source)

WORKPLACE VIOLENCE

Vendor Working For Kroger Grocery Store Who Was Asked To Leave Store Kills 1 Person / Leaves 14 Wounded - September 23, 2021

The shooter moved into the Town of Collierville, in Tennessee, during the summer of 2020. He was a third-party vendor working inside Kroger and was asked to leave his job the morning of Thursday, September 23, 2021. The alleged shooter, 29-year-old UK Thang, died of an apparent self-inflicted gunshot wound.

The deceased victim was identified as Olivia King, who was a customer at the store. 10 employees and 4 other customers were wounded. Police said only 4 victims remain at Regional One Hospital, all of whom are in stable condition. (Source)

Employee Who Threatened Violent Shooting At Workplace Sentenced To Prison For Being A Felon In Possession Of A Firearm - September 23, 2021

Michael Ammons made comments to coworkers in April 2021 threatening to "go postal" and "shoot up the place" at a trucking company where he was employed. Federal agents responded to the business and detained Ammons, who admitted to making the threatening statements. During a later search of Ammons's residence, agents recovered a .40-caliber pistol and .22-caliber long rifle bullets. Ammons admitted to possessing the pistol and the bullets. He also acknowledged that, as a convicted felon, he was not allowed to be in possession of a firearm or ammunition. (Source)

PREVIOUS INSIDER THREAT INCIDENT REPORTS

https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEES WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

Former Controller Of Oil & Gas Company Sentenced To Prison For $65 Million Bank Fraud Scheme Over 21 Years / 275 Employees Lost Jobs – (2016)

In September 2020, Judith Avilez, the former Controller of Worley & Obetz, pleaded guilty to her role in a scheme that defrauded Fulton Bank of over $65 million. Avilez admitted that from 2016 through May 2018, she helped Worley & Obetz's CEO, Jeffrey Lyons, defraud Fulton Bank by creating fraudulent financial statements that grossly inflated accounts receivable for Worley & Obetz's largest customer, Giant Food. Worley & Obetz was an oil and gas company in Manheim, PA, that provided home heating oil, gasoline, diesel, and propane to its customers.

Lyons initiated the fraud shortly after he became CEO in 1999. In order to make Worley & Obetz appear more profitable and himself appear successful as the CEO, Lyons asked the previous Worley & Obetz Controller, Karen Connelly, to falsify the company's financial statements to make it appear to have millions more in revenue and accounts receivable than it did.

Lyons and Connelly continued the fraud scheme from 2003 until 2016, when Connelly retired and Avilez became the Controller and joined the fraud. Avilez and Lyons continued the scheme in the same manner that Lyons and Connelly had. Each month, Avilez created false Worley & Obetz financial statements that Lyons presented to Fulton Bank in support of his request for additional loans or extensions on existing lines of credit. In total, Lyons, Connelly, and Avilez defrauded Fulton Bank out of $65,000,000 in loans.

After the scheme was discovered, Worley & Obetz and its related companies did not have the assets to repay the massive amount of Fulton loans Lyons had accumulated.

In June 2018, Worley & Obetz declared bankruptcy and notified its approximately 275 employees that they no longer had jobs. After 72 years, the Obetz's family-owned company closed its doors forever.

The fraud Lyons committed with the help of Avilez and Connelly caused many families in the Manheim community to suffer financially and emotionally. Fulton Bank received some repayments from the bankruptcy proceedings but is still owed over $50,000,000. (Source)

Former Engineering Supervisor Costs Company $1 Billion In Shareholder Equity / 700 Employees Lost Jobs (2011)

AMSC formed a partnership with Chinese wind turbine company Sinovel in 2010. In 2011, an Automation Engineering Supervisor at AMSC secretly downloaded AMSC source code and turned it over to Sinovell. Sinovel then used this same source code in its wind turbines.

2 Sinovel employees and 1 AMSC employee were charged with stealing proprietary wind turbine technology from AMSC in order to produce their own turbines powered by stolen intellectual property.

Rather than pay AMSC for more than $800 million in products and services it had agreed to purchase, Sinovel instead hatched a scheme to brazenly steal AMSC's proprietary wind turbine technology, causing the loss of almost 700 jobs which accounted for more than half of its global workforce, and more than $1 billion in shareholder equity at AMSC. (Source)

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

Former Employee Sentenced To Prison For Sabotaging Cisco's Network With Damages Costing $2.4 Million (2018)

Sudhish Ramesh admitted to intentionally accessing Cisco Systems' cloud infrastructure that was hosted by Amazon Web Services without Cisco's permission on September 24, 2018.

Ramesh worked for Cisco and resigned in approximately April 2018. During his unauthorized access, Ramesh admitted that he deployed a code from his Google Cloud Project account that resulted in the deletion of 456 virtual machines for Cisco's WebEx Teams application, which provided video meetings, video messaging, file sharing, and other collaboration tools. He further admitted that he acted recklessly in deploying the code, and consciously disregarded the substantial risk that his conduct could harm to Cisco.

As a result of Ramesh's conduct, over 16,000 WebEx Teams accounts were shut down for up to two weeks, and caused Cisco to spend approximately $1,400,000 in employee time to restore the damage to the application and refund over $1,000,000 to affected customers. No customer data was compromised as a result of the defendant's conduct. (Source)

IT Systems Administrator Receives Poor Bonus And Sabotages 2000 IT Servers / 17,000 Workstations - Cost Company $3 Million+ (2002)

A former system administrator that was employed by UBS PaineWebber, a financial services firm, infected the company's network with malicious code. He was apparently irate about a poor salary bonus he received of $32,000. He was expecting $50,000.

The malicious code he used is said to have cost UBS $3.1 million in recovery expenses and thousands of lost man hours.

The malicious code was executed through a logic bomb which is a program on a timer set to execute at predetermined date and time. The attack impaired trading, while impacting over 2,000 servers and 17,000 individual workstations in the home office and 370 branch offices. Some of the information was never fully restored.

After installing the malicious code, he quit his job. Following, he bought puts against UBS. If the stock price for UBS went down, because of the malicious code for example, he would profit from that purchase. (Source)

Hackers Looking To Pay $1 Million+ For Disgruntled Employees To Deploy Ransomware Within Employers Networks (2021)

Criminal hackers will try almost anything to get inside a profitable enterprise and secure a million-dollar payday from a ransomware infection. Apparently now that includes emailing employees directly and asking them to unleash the malware inside their employer's network in exchange for a percentage of any ransom amount paid by the victim company.

Crane Hassold, director of threat intelligence at Abnormal Security, described what happened after he adopted a fake persona and responded to hackers proposal. It offered to pay him
40% of a million-dollar ransom demand if he agreed to launch their malware inside his employer's network.

Abnormal Security documented how it tied the email back to a young man in Nigeria who acknowledged he was trying to save up money to help fund a new social network he is building called Sociogram. (Source)

Former Human Resources Manager Convicted Of Deleting Over 17,000 Files (All Of Employers Data) While Being Terminated (2021)

In January 2019, Medghyne Calonge was hired by an online provider of professional services. She was to serve as the head of human resources.

On June 28, 2019, Calonge as terminated for failing to meet the minimum requirements of her job after, among other things, she improperly downgraded a colleague's access to a computer system following an argument with the colleague.

While she was being terminated, and just before she was escorted from the building, Calonge was observed by 2 employees of repeatedly hitting the delete key on her desktop computer. Hours later she logged into a system which the company had invested 2 years and over $100,000 to build. During the next 2 days, she deleted over 17,000 job applications and resumes, and left messages with profanities inside the system. She completely destroyed all her employers data. (Source)

Hackers Looking To Pay $1 Million+ For Disgruntled Employees To Deploy Ransomware Within Employers Networks (2021)

Criminal hackers will try almost anything to get inside a profitable enterprise and secure a million-dollar payday from a ransomware infection. Apparently now that includes emailing employees directly and asking them to unleash the malware inside their employer's network in exchange for a percentage of any ransom amount paid by the victim company.

Crane Hassold, director of threat intelligence at Abnormal Security, described what happened after he adopted a fake persona and responded to hackers proposal. It offered to pay him
40% of a million-dollar ransom demand if he agreed to launch their malware inside his employer's network.

Abnormal Security documented how it tied the email back to a young man in Nigeria who acknowledged he was trying to save up money to help fund a new social network he is building called Sociogram. (Source)

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

Produced By: National Insider Threat Special Interest Group / Insider Threat Defense Group

The websites listed below are updated monthly with the latest incidents.

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**2,900+ Incidents**).

View On This Link. Or Download The Flipboard App To View On Your Mobile Device

https://flipboard.com/@cybercops911/insider-threat-incidents-magazine-resource-guide-tkh6a9b1z

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

(**500+ Incidents**)

https://www.insiderthreatdefense.us/category/insider-threat-incidents/

Incident Posting Notifications

Enter your e-mail address in the Subscriptions box on the right of this page.

https://www.insiderthreatdefense.us/news/

INSIDER THREAT INCIDENTS COSTING $1 MILLION TO $1 BILLION +

https://www.linkedin.com/post/edit/6696456113925230592/

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

https://twitter.com/InsiderThreatDG

Follow Us On Twitter: @InsiderThreatDG

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

https://www.nationalinsiderthreatsig.org/crticial-infrastructure-insider-threats.html

National Insider Threat Special Interest Group (NITSIG)

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center. The mission of the NITSIG is to provide organizations and individuals with a ***central source*** for Insider Threat Mitigation (ITM) guidance and collaboration.

The NITSIG Membership (**Free**) is the largest network (**1000+**) of ITM professionals in the U.S. and globally. We our proud to be a conduit for the collaboration of ITM information, so that our members can share and gain information and contribute to building a common body of knowledge for ITM. Our member's willingness to share information has been the driving force that has made the NITSIG very successful.

The NITSIG Provides Guidance And Training The Membership And Others On;

- ✓ Insider Threat Program (ITP) Development, Implementation & Management
- ✓ ITP Working Group / Hub Operation
- ✓ Insider Threat Awareness and Training
- ✓ ITM Risk Assessments & Mitigation Strategies
- ✓ User Activity Monitoring / Behavioral Analytics Tools (Requirements Analysis, Guidance)
- ✓ Protecting Controlled Unclassified Information / Sensitive Business Information
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

The NITSIG has meetings primarily held at the John Hopkins University Applied Physics Lab in Laurel, Maryland and other locations (NITSIG Chapters, Sponsors). There is **NO CHARGE** to attend. See the link below for some of the great speakers we have had at our meetings.
http://www.nationalinsiderthreatsig.org/nitsigmeetings.html

The NITSIG has created a Linked Group for individuals that interested in sharing and gaining in-depth knowledge regarding ITM and Insider Threat Program Management (ITPM). This group will also enable the NITSIG to share the latest news, upcoming events and information for ITM and ITPM. We invite you to join the group. https://www.linkedin.com/groups/12277699

The NITSIG is the creator of the "***Original***" Insider Threat Symposium & Expo (ITS&E). The ITS&E is recognized as the ***Go To Event*** for in-depth real world guidance from ITP Managers and others with extensive ***Hands On Experience*** in ITM.

At the expo are many great vendors that showcase their training, services and products. The link below provides all the vendors that exhibited at the 2019 ITS&E, and provides a description of their solutions for Insider Threat detection and mitigation.
https://nationalinsiderthreatsig.org/nitsiginsiderthreatvendors.html

The NITSIG had to suspend meetings and the ITS&E in 2020 due to the COVID outbreak. We are working on resuming meetings in the later part of 2021, and looking at holding the ITS&E in 2022.

NITSIG Insider Threat Mitigation Resources
Posted on the NITSIG website are various documents, resources and training that will assist organizations with their Insider Threat Program Development / Management and Insider Threat Mitigation efforts.
http://www.nationalinsiderthreatsig.org/nitsig-insiderthreatsymposiumexporesources.html

Security Behind The Firewall Is Our Business

The Insider Threat Defense (ITDG) Group is considered a ***Trusted Source*** for Insider Threat Mitigation (ITM) training and consulting services to the U.S. Government, Department Of Defense, Intelligence Community, United States Space Force, Fortune 100 / 500 companies and others; Microsoft Corporation, Walmart, Home Depot, Nike, Tesla Automotive Company, Dell Technologies, Discovery Channel, Symantec Corporation, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines, Universities, Law Enforcement and many more.

The ITDG has provided training and consulting services to over **640+** organizations. (Client Listing)

Over **875+** individuals have attended our highly sought after Insider Threat Program (ITP) Development / Management Training Course (Classroom Instructor Led & Live Web Based) and received ITP Manager Certificates. (Training Brochure)

With over 10+ years of experience providing training and consulting services, we approach the Insider Threat problem and ITM from a realistic and holistic perspective. A primary centerpiece of providing our clients with a comprehensive ITM Framework is that we incorporate lessons learned based on our analysis of ITP's, and Insider Threat related incidents encountered from working with our clients.

Our training and consulting services have been recognized, endorsed and validated by the U.S. Government and businesses, as some of the most ***affordable, comprehensive and resourceful*** available. These are not the words of the ITDG, but of our clients. ***Our client satisfaction levels are in the exceptional range***. We encourage you to read the feedback from our students on this link.

ITDG Training / Consulting Services Offered

Training / Consulting Services (Conducted Via Live Instructor Led Classroom / Onsite / Web Based)

- ✓ ITM Training Workshops For CEO's, C-Suite & ITP Managers / Working Group, Insider Threat Analysts & Investigators
- ✓ ITP Development - Management / ITM / Insider Threat Investigator & Related Training Courses
- ✓ ITM Framework Training (For Organizations Not Interested In Developing An ITP)
- ✓ Insider Threat Vulnerability - ITP Maturity Assessment / Mitigation Guidance
- ✓ Malicious Insider Playbook Of Tactics Assessment / Mitigation Guidance
- ✓ Insider Threat Awareness Training For Employees
- ✓ Insider Threat Detection Tool Guidance / Pre-Purchasing Evaluation Assistance
- ✓ Customized ITM Consulting Services For Our Clients

For additional information on our training, consulting services and noteworthy accomplishments please visit this link.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program (ITP) Development / Management Training Course Instructor
Insider Threat Vulnerability - ITP Maturity Assessment / Mitigation Specialist
Insider Threat Researcher / Speaker
Founder / Chairman Of The National Insider Threat Special Interest Group (NITSIG)
NITSIG Insider Threat Symposium & Expo Director / Organizer
888-363-7241 / 561-809-6800
www.insiderthreatdefense.us / james.henderson@insiderthreatdefense.us
www.nationalinsiderthreatsig.org / jimhenderson@nationalinsiderthreatsig.org