2024 INSIDER THREAT INCIDENTS REPORT FOR THE DEPARTMENT OF DEFENSE

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

Current Service Members / Veterans

The National Insider Threat Special Interest Group (NITSIG), NITSIG Members & the Insider Threat Defense Group
Thank You For Your Service.

We express our sincere gratitude and admiration for U.S. active service members and veterans, for your dedication to the USA, and the sacrifices you have made, such as putting yourselves in harm's way, giving up time with loved ones, and for those service members who have given the ultimate sacrifice and have died in service, while protecting the country's freedoms.

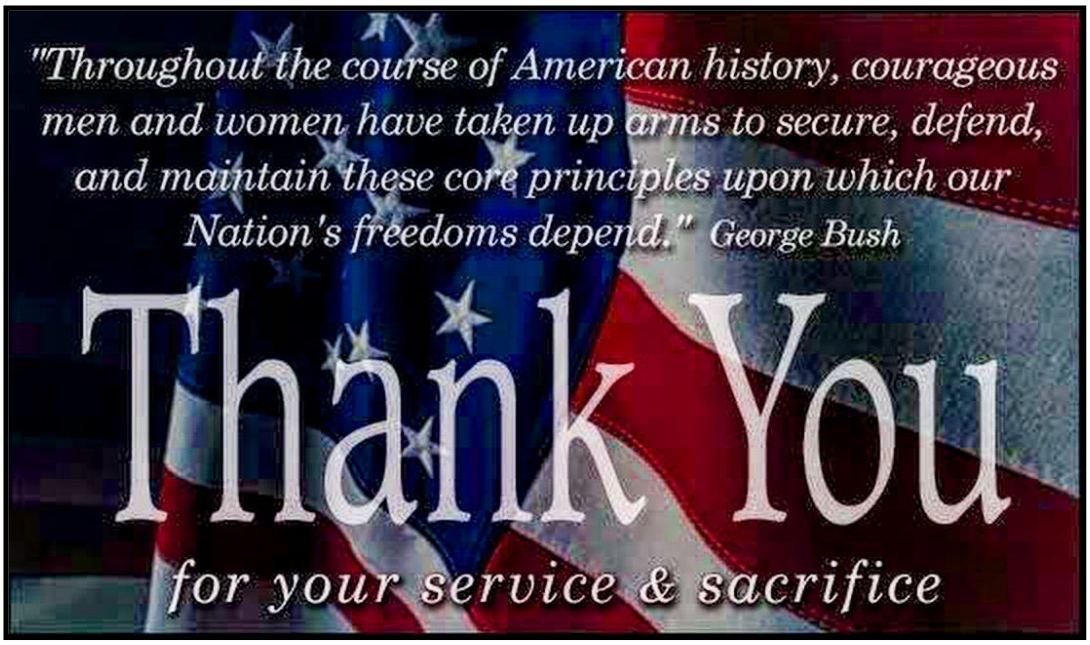


TABLE OF CONTENTS

INSIDER THREAT INCIDENTS

A Very Costly And Damaging Problem

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) has conducted extensive research on the Insider Threat problem for 15+ years. This research has evaluated and analyzed over **5,400+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents. These monthly report provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes.

Insider Threat incidents within the Department of Defense (DoD) (U.S. Army, Navy, Air Force, Marines) are not just related to espionage, the unauthorized distribution of classified information to foreign governments or other individuals, or the prevalence of extremist ideology and behaviors.

The traditional norm or mindset that DoD employees just steal classified information or other sensitive information is no longer the case. There continues to be an increase within the DoD of financial fraud, contracting fraud, bribery, kickbacks, theft of DoD physical assets, etc. This is very evident in the research that has been conducted by the NITSIG.

While some employees may display behavioral indicators of concerns, some may not. Other employees are apparently motivated by human greed, the need for more money, or the opportunity to live a lifestyle of luxury at the expense of the DoD. Perpetrators have used DoD money for: Investment Ventures, To Pay Debts, Jewelry, Clothing, Vehicles, Real Estate, Vacations and more.

DoD organizations have invested millions of dollars in securing their data, computers and networks against Insider Threats, from primarily a technical perspective, using Network Security Tools or Insider Threat Detection Tools. But the Insider Threat problem is not just a technical problem.

Just putting an Insider Threat Program (ITP) is place and purchasing expensive employee monitoring tools, does not always stop Insiders Threat incidents from happening, if these monitoring tools **are not designed** to detect the malicious actions of employees who may use **low tech methods** as referenced in the below report.

DoD 2019 PERSERC Report Summary - Data Exfiltration Project

The objective of this study was to identify common themes and behavioral indicators that preceded individuals' arrests in order to prevent and mitigate future incidents. In total, 83 cases of DoD data exfiltration were included in this study, and researchers collected information related to 392 variables of interest, to include pre-arrest behavior that matched disqualifying factors of the Adjudicative Guidelines and / or behavioral threat assessment themes.

The report states that to remove resources, perpetrators most often **carried them out the door** of a secure facility, usually concealed in an everyday object such as a bag or briefcase. Among those who transmitted material to a foreign entity, Russia was the most common recipient. The most common motive was money, followed by ideology. (Source)

The Human Operating System (Brain) is very sophisticated and underestimating the motivations and capabilities of a malicious or opportunist employee can have severe impacts for DoD organizations. Insider Threat Mitigation (ITM) requires "**Thinking Outside The Box**".

Don't forget that Insiders know about your organizations security controls, and how they might be able to work around them, to achieve their malicious objectives. A malicious Insider may be conducting their own security assessment to determine the best method to achieve their objectives, before the organization discovers the vulnerabilities. Being proactive in identifying security weaknesses and vulnerabilities, **rather then reactive** is a critical component for ITM. Has your DoD organization conducted a Data Exfiltration Assessment to test the security posture of your facility?

An ITP is a requirement for DoD organizations to support and enhance their ITM efforts.

But mitigating Insider Threats IS NOT something new in the DoD. The DoD wrote a report in 1998 named DoD Insider Threat Mitigation (ITM). This report provided an explicit set of recommendations for actions to mitigate the Insider Threat to DoD information systems. **The report cited an "Urgent need to get back to the basics by supporting existing policy. Insistence that existing policy and procedures must be observed and should be DoD's very valuable first step to ITM."** (Source)

It is 2024. Ensuring comprehensive and robust security policies and controls are in place and functioning property within the DoD, are still as important as when the above report was written.

Creating an ITP is the new approach for identifying, preventing and mitigating employee risks and threats within the DoD. This concept was outlined in Executive 13587 (Released 2011) and National Insider Threats Policy (Released 2012).

But just because DoD organizations (Commands, Services, Agencies) have an ITP and conduct MANY Insider Threat investigations, does not simply mean they have an effective ITP.

Support from Counterintelligence is critical and is needed to support Insider Threat Investigations within the DoD. But Insider Threats is not just Counterintelligence problem. There are many other departments and key stakeholders that also play a big part in ITM. These individuals include but are not limited to: Insider Threat Analyst, FSO, Personnel Security, Force Protection, CIO - IT, Network Security, Mental Health / Behavioral Science Professionals, Legal Etc.)

Having an ITP is not just about conducting investigations. ITM starts with being proactive and focusing on prevention and mitigation techniques. An ITP Manager must work with key stakeholders and departments to ensure polices and procedures within various departments are in place to prevent or mitigate employee risks / threats.

The ITP Manager must work closely with key stakeholders to ensure they have a much broader and deeper understanding of the collaboration required, and the many critical components that are essential for a comprehensive ITP. This will ensure key stakeholders are **universally aligned** from an enterprise / holistic perspective to identify, prevent or mitigate employee risks / threats.

Posted on the Director of National Intelligence website is a document that outlines when an ITP reaches Full Operating Capability, by implementing all 26 minimum standards. (Source 1, Source 2)

What is not listed in this document is the requirement to ensure DoD organizations have done a comprehensive review of their security foundations and internal fraud controls to ensure there are no weaknesses or vulnerabilities. This review would be done from an enterprise approach that covers evaluating security controls and internal fraud controls from a non-technical and technical perspective. (Identify, Prevent Or Mitigate)

Judging by the many incidents within the DoD that are related to financial fraud, contracting fraud, bribery, theft of assets, etc. as outlined in this report, it appears more internal fraud controls and other security controls may be needed.

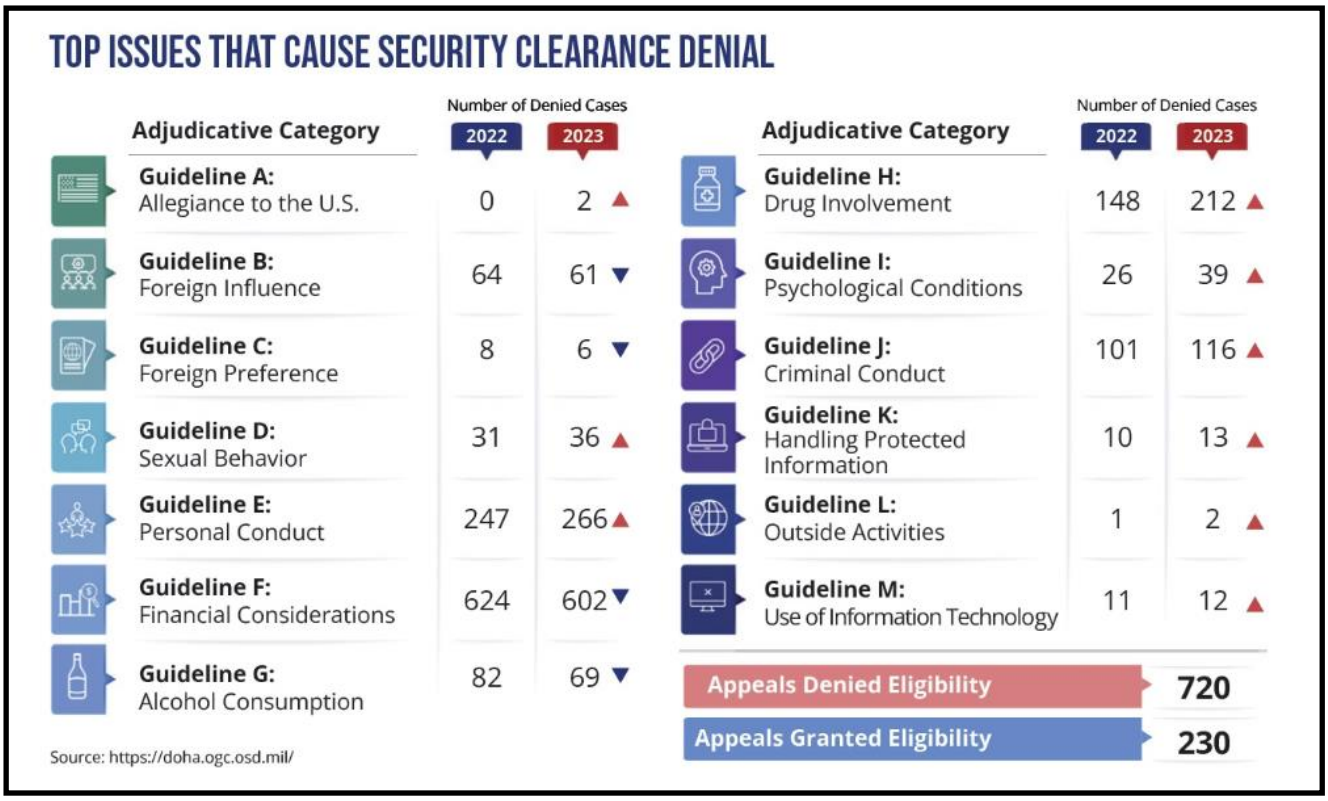
The intent of this report is to provide a more holistic view of various types of Insider Threat incidents within the DoD.

This report should be used as an awareness and educational tool to gain support from senior leaders for additional funding for ITP's.

This report also serves as an excellent Insider Threat Awareness Tool, to educate key stakeholders supporting an ITP, and to educate DoD employees on the importance of reporting employees' who may pose a risk or threat to the organization.

What Are The Top Causes Of Security Clearance Denial & Revocation In 2023?

Financial Considerations



DOD INSIDER THREAT INCIDENTS

2020 To 2024

U.S. Army Civilian Employee Sentenced To Prison For $100 Million Fraud Scheme / Used Funds For Jewelry, Clothing, Vehicles, Real Estate - - July 23,2024

Janet Mello worked as a Financial Program Manager for the U.S. Army, Installation Management Command – G9 (Morale, Welfare and Recreation) Child and Youth Services (CYS) at Fort Sam Houston, in Texas

In or around December 2016 through at least August 29, 2023, Mello formed a business she called Child Health and Youth Lifelong Development (CHYLD). The sole purpose of CHYLD was to receive grant funds from the 4-H Military Partnership Grant program, which Mello fraudulently secured by way of her position as a CYS financial program manager.

Once Mello received a grant check, she deposited the check into her bank account, spending the money on clothing, jewelry, vehicles and real estate. Mello repeated the process 49 times during a six-year period, requesting approximately $117,000,000 in payments, and receiving approximately $108,917,749. (Source)

U.S. Army Reserve Officer Admits To Military Pay Fraud Of $140,000+ - July 19, 2024

Captain Jean Philippe Martial worked as a U.S. Army Reservist from Utah's 76th Operational Response Command. He was indicted for military pay fraud that occurred at Fort Douglas, Utah, during the coronavirus pandemic.

Captain Martial defrauded the United States out of more than $140,000 in unearned military pay entitlements from June 2019 to September 2021. Last month, Colonel Reece Roberts, formerly of Utah's 76th Operational Response Command, pled guilty to filing a fraudulent claim against the United States, conspiring to defraud the United States, and other federal crimes. (Source)

Employee Of DoD Armed Forces Recreation Center Pleads Guilty Theft Of $183,000+ - July 9, 2024

Elizabeth Carpenter was employed as an accounting technician by Shades of Green, an Armed Forces Recreation Center resort owned by the Department of Defense (DOD) located on Walt Disney World Resort property in Lake Buena Vista.

Between July 13, 2022, and March 19, 2024, Carpenter used her position as a DOD employee with computer credentials to access guest accounts to refund a portion of guests' room payments to Carpenter's personal credit card accounts. Carpenter engaged in at least 652 unauthorized transactions totaling approximately $183,079. (Source)

National Security Agency Contractor Sentenced To Prison For $176,000+ Time & Attendance Fraud - July 3, 2024

Jacky McComber was the Chief Executive Officer of an information technology company that had contracts with the NSA. Because the subject matter of these contracts involved classified information, most of the work had to be performed at a secure location, and there were significant limitations to the amount of work that could be performed off-site.

McComber billed for her supposed work physically at the NSA, when in reality approximately 90% of the work she billed for was not when she physically was at the NSA.

The evidence further showed that McComber at times did not work the number of hours on the contract that she recorded on her timesheets. For example, on occasions when McComber billed a full day to the contract, she participated in charity events, attended a reunion, and was on vacation. As further detailed in trial testimony, McComber participated in a voluntary interview with NSA-OIG investigators as a result of information received from a whistleblower indicating that McComber was billing the government for hours that she was not actually working.

McComber was odered to pay $176,913 in restitution for submitting false invoices to the National Security Agency (NSA) for overstating her hours worked on a contract and for making false statements to investigators from the NSA's Office of the Inspector General. (Source)

DoD Employee Pleads Guilty To $624,000 Fake Invoices Scheme - July 1, 2024

Zelene Charles, a previous civilian employee of the Department of Defense, at the Defense Language Institute in Monterey, California, perpetrated a scheme to defraud the U.S. government by creating fake purchase requests and invoices for government purchases from both fictitious and legitimate business entities.

The items listed in these invoices were never actually purchased or received by the government. Between December 2016 and April 2020, Charles placed approximately 185 fraudulent charges, causing a total loss to the government of $624,250. To conceal that she was the recipient of the stolen funds, Charles frequently renamed the business names associated with intermediary accounts and, in total, used at least 78 different account names. (Source)

U.S. Army Research Biologist Pleads Guilty To Accepting $40,000 In Bribes In Exchange For Favorable Action on Contracts - July 1, 2024

Jason Edmonds was employed by the United States Army as a Research Biologist at the U.S. Army Combat Capabilities Development Command (CCDC) Chemical Biological Center (CB Center) located at the Aberdeen Proving Ground (APG) in Marylan. The CCDC CB Center was the nation's principal research and development center for non-medical chemical and biological weapons defense. The CB Center developed technology in the areas of detection, protection, and decontamination.

From 2012 to 2019, Edmonds accepted cash and other financial benefits from John Conigliaro, the owner and CEO of EISCO, Inc. in exchange for favorable action on CB Center contracts. For example, in July 2013, Edmonds directed a $300,000 CB Center project to EISCO. Three months later, in October 2013, Conigliaro gave Edmonds $40,000 in cash so that Edmonds could purchase two rental real estate properties. Once Edmonds purchased the rental properties, Conigliaro paid for thousands of dollars of renovations to the rental properties.

Relative to the cash exchange, Edmonds and Conigliaro executed a "Promissory Note," which was subsequently amended by Edmonds on June 14, 2014. In the amended "Promissory Note," Edmonds credited himself $18,100 against the $40,000 in cash for past projects that Edmonds had directed to EISCO at the CB Center. Edmonds also wrote that Conigliaro would provide him an additional $25,000 in exchange for future projects that Edmonds would direct to EISCO.

Between December 2016 and August 2017, Edmonds directed a series of government projects to EISCO in exchange for a stream of benefits from Conigliaro, including a kitchen remodel at Edmonds's personal residence, the purchase of a granite countertop, a kitchen sink, and new siding to his home. (Source)

U.S. Navy Civilian Employee Pleads Guilty To Bribery Scheme Involving $100 Million+ In Government Contracts To Live Luxury Lifestyle - June 12, 2024

James Soriano is a former civilian employee of the San Diego based Naval Information Warfare Center (NIWC).

Soriano pleaded guilty to multiple bribery conspiracies, admitting that while he was a public official at NIWC, he accepted hundreds of thousands of dollars from defense contractors in the form of free meals, tickets to premier sporting events, jobs for family and friends, and other things, in exchange for helping those contractors win and maintain hundreds of millions of dollars in government contracts.

From approximately March 2016 through at least October 2019, Soriano and a coworker, Dawnell Parker, received bribes from Philip Flores, the President and CEO of Intellipeak Solutions, Inc., a defense contractor headquartered in Fredericksburg, Virginia.

Soriano also admitted that from approximately May 2015 through at least October 2019, he and Parker separately received bribes from another defense contractor, with offices in San Diego and Stafford, Virginia, who also gave him things of value, such as expensive meals, a job for his wife, and rounds of golf at private country clubs.

From approximately June 2014 through at least October 2019, Soriano received bribes from Russell Thurston, the Vice President of Cambridge International Systems, Inc., a defense contractor headquartered in Arlington, Virginia. In return for these bribes, Soriano used various methods to steer contracts to these defense contractors and kept his contracting activities hidden from the Naval Information Warfare Center.

According to Soriano's plea agreement, the defense contractors acting through their presidents, officers, and employees gave various things of value to Soriano, including dinners at Ruth's Chris, Island Prime, and Providence; tickets to the 2018 MLB All-Star Game, 2018 World Series, and 2019 Superbowl; and jobs for Soriano's family and friends, including a member of Soriano's family and Soriano's family friend, Liberty Gutierrez, who was giving Soriano $2,000 a month from her salary at one of the companies working under a defense contract. (Source)

U.S. Navy Admiral (Now Retired) & Business Executives Arrested In Connection With Alleged Bribery Scheme - May 31, 2024

From 2020 to 2022, Robert Burke was a four-star Admiral who oversaw Naval operations in Europe, Russia, and most of Africa, and commanded thousands of civilian and military personnel.

Yongchul "Charlie" Kim and Meghan Messenger were the co-CEOs of a company (Company A) that provided a workforce training pilot program to a small component of the Navy from August 2018 through July 2019. The Navy terminated a contract with Company A in late 2019 and directed Company A not to contact Burke.

Despite the Navy's instructions, Kim and Messenger then allegedly met with Burke in Washington, D.C., in July 2021, in an effort to reestablish Company A's business relationship with the Navy. At the meeting, the charged defendants allegedly agreed that Burke would use his position as a Navy Admiral to steer a sole-source contract to Company A in exchange for future employment at the company. They allegedly further agreed that Burke would use his official position to influence other Navy officers to award another contract to Company A to train a large portion of the Navy with a value Kim allegedly estimated to be "triple digit millions."

In furtherance of the conspiracy, in December 2021, Burke allegedly ordered his staff to award a $355,000 contract to Company A to train personnel under Burke's command in Italy and Spain. Company A performed the training in January 2022.

Thereafter, Burke allegedly promoted Company A in a failed effort to convince a senior Navy Admiral to award another contract to Company A. To conceal the scheme, Burke allegedly made several false and misleading statements to the Navy, including by creating the false appearance that Burke played no role in issuing the contract and falsely implying that Company A's employment discussions with Burke only began months after the contract was awarded.

In October 2022, Burke began working at Company A at a yearly starting salary of $500,000 and a grant of 100,000 stock options.

Burke, Kim, and Messenger are each charged with conspiracy to commit bribery and bribery. Burke is also charged with performing acts affecting a personal financial interest and concealing material facts from the United States. If convicted, Burke faces a maximum penalty of 30 years in prison, and Kim and Messenger each face a maximum penalty of 20 years in prison. (Source)

U.S. Navy $35 Million Contract & Bribery Scandal Involving 1000 Navy Officers / 91 Admirals Is Now Facing Legal Problems For Prosecution - May 23, 2024

Leonard Glenn Francis, better known as "Fat Leonard," is a 6 feet, 3 inch tall, 350 pound former Malaysian defense contractor who bribed hundreds of Navy officers for classified information for more than 20 years. He eventually defrauded the U.S. government and American taxpayers out of at least $35 million dollars until he was caught in a sting operation in 2013. After Francis' arrest, nearly 1,000 Navy officers came under scrutiny, including 91 admirals. Federal prosecutors brought criminal charges against 34 defendants.

In what has become one of the largest scandals in U.S. Navy history, Francis bribed the Navy officers with lavish meals, expensive gifts, prostitutes and orgies.

The officers looked the other way as he grossly overcharged on U.S. Navy contracts for his Singapore-based maritime services supply company, Glenn Defense Marine Asia Ltd., which supplied food, water and fuel to U.S. Navy assets.

A San Diego judge recently dismissed the felony convictions for five military officers who admitted to accepting bribes from Francis. The convictions were dismissed at the request of the government due to "prosecutorial errors."

Francis' bribing did not stop when he was arrested. Later hospitalized and treated for cancer, he convinced the judge to let him go on house arrest to have a more comfortable recovery. In 2022, he cut off his GBS tracker and called an Uber to escape house arrest. He ended up in Tijuana, Mexico, and eventually made his way to Venezuela, where he was captured and sent back to the U.S. in a prisoner swap in December 2023. Prosecutors are waiting until Francis is sentenced to bring charges related to his escape. (Source)

U.S. Army Lieutenant Colonel Charged With Arms Export Control Act Violations - May 3, 2024

Frank Talbert is a Lieutenant Colonel with U.S. Army Explosives Ordinance Disposal (EOD) assigned to Fort Campbell.

He is facing federal criminal charges after law enforcement officers conducted an investigation and executed multiple search warrants uncovering evidence that Talbert unlawfully imported firearms parts from Russia and other countries, unlawfully dealt in firearms without a federal firearms license, and committed multiple firearms violations related to the possession of machineguns. (Source)

U.S. Army Major Found Guilty After Smuggling Guns To Ghana - April 29, 2024

A federal jury convicted a United States Army Major (Kojo Dartey), currently assigned to Fort Liberty, on charges of dealing in firearms without a license, delivering firearms without notice to the carrier, smuggling goods from the United States, illegally exporting firearms without a license, making false statements to an agency of the United States, making false declarations before the court, and conspiracy.

Between June 28 and July 2, 2021, Dartey purchased seven firearms in the Fort Liberty area and tasked a U.S. Army Staff Sergeant at Fort Campbell, Kentucky, to purchase three firearms there and send them to Dartey in North Carolina. Dartey then hid all the firearms, including multiple handguns, an AR15, 50-round magazines, suppressors, and a combat shotgun inside blue barrels underneath rice and household goods and smuggled the barrels out of the Port of Baltimore, Maryland, on a container ship to the Port of Tema in Ghana. The Ghana Revenue Authority recovered the firearms and reported the seizure to the DEA attaché in Ghana and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Baltimore Field Division. At the same time, Dartey was a witness in the trial of U.S. v. Agyapong.

A case that involved a 16-defendant marriage fraud scheme between soldiers on Fort Liberty and foreign nationals from Ghana that Dartey had tipped off officials to. In preparation for the trial, Dartey lied to federal law enforcement about his sexual relationship with a defense witness and lied on the stand and under oath about the relationship. (Source)

U.S. Army Reservist Sentenced To Prison For Theft Of $11,000+ From Government - April 26, 2024

Leroy Daniels stole $11,693.87 from the United States Department of the Army by claiming reimbursement for the performance of military funeral honors ceremonies that never occurred. (Source)

U.S. Army Service Member Sentenced To Prison In Money Laundering Romance Scam - April 18, 2023

Sanda Frimpong, wa an active duty service member stationed at Fort Bragg.

Frimpong was arrested after the unsealing of a 19-count indictment that included charges of Money Laundering, Fraud, Conspiracy, Aggravated Identity Theft, and Access Device Fraud in connection with multiple interstate and international fraud and money-laundering scams.

Frimpong and other conspirators, engaged in elaborate scams, impersonating romantic love interests, diplomats, customs personnel, military personnel, and other fictitious personas for the purpose of ensnaring their victims by earning their confidence, including promises of romance, sharing of an inheritance or other riches, or other scenarios intended to fraudulently induce the victims to provide money or property to the conspirators.

Frimpong allegedly laundered hundreds of thousands of dollars in proceeds of these frauds through his various bank accounts across state lines and through contacts in Ghana. (Source)

U.S. Army Financial Counselor Admits To Defrauding Families Through Investment Scheme Which Earned Him $1.4 Million In Commissions - April 16, 2024

From November 2017 to January 2023, Caz Craffy was a civilian employee of the U.S. Army, working as a financial counselor with the Casualty Assistance Office. He was also a Major in the U.S. Army Reserves, where he has been enlisted since 2003. Craffy was responsible for providing general financial education to the surviving beneficiaries. He was prohibited from offering any personal opinions regarding the surviving beneficiary's benefits decisions.

Craffy was not permitted to participate personally in any government matter in which he had an outside financial interest. However, without telling the Army, Craffy simultaneously maintained outside employment with two separate financial investment firms.

Craffy used his position as an Army financial counselor to identify and target Gold Star families and other military families. He encouraged the Gold Star families to invest their survivor benefits in investment accounts that he managed in his outside, private employment. Based upon Craffy's false representations and omissions, the vast majority of the Gold Star families mistakenly believed that Craffy's management of their money was done on behalf of and with the Army's authorization.

From May 2018 to November 2022, Craffy obtained more than $9.9 million from Gold Star families to invest in accounts managed by Craffy in his private capacity. Once in control of this money, Craffy repeatedly executed trades, often without the family's authorization. These unauthorized trades earned Craffy high commissions.

During the timeframe of the alleged scheme, the Gold Star family accounts had lost more than $3.7 million, while Craffy personally earned more than $1.4 million in commissions, drawn from the family accounts. (Source)

U.S. Army Reserve Officer Pleads Guilty To $488,000+ COVID Relief Fraud Scheme / Used Funds For Investment Ventures & To Pay Debts - March 6, 2024

Russell Laraway, an Army Reserve officer, incorporated two business entities in Virginia that he purported to operate out of his home in Leesburg: Loudoun Innovation LLC (LI LLC) and Commonwealth Commerce LLC (CC LLC).

Beginning in April 2020, Laraway submitted loan applications through the Paycheck Protection Program (PPP), a COVID-19 relief program that was intended to provide loans backed by the Small Business Administration to certain businesses, nonprofit organizations, and other entities to help them retain their employees or stay afloat during the pandemic. In his applications, Laraway inflated the numbers of people his business entities employed and falsified payroll expenses and revenues for each company.

Laraway sought loan forgiveness for some of the PPP loans by falsely certifying that the PPP money had been used solely for payroll or other authorized purposes, while he actually intended to use the money to engage in spurious investment ventures and pay off personal debts. Laraway fraudulently received two PPP loans for LI LLC and two PPP loans for CC LLC. The four PPP loans totaled approximately $488,952, some of which Laraway paid to foreign entities in scams of which he was a victim. (Source)

2 U.S. Marines And Nurse Practitioner Sentenced To Prison For $65 Million+ TRICARE Military Healthcare Program Fraud Scheme - February 16, 2024

Three members of a massive conspiracy to bilk the military's healthcare program known as TRICARE out of more than $65 million have been sentenced to prison in federal court.

Former U.S. Marines, Daniel Castro and Jeremy Syto, were sentenced to 21 months and 15 months. Nurse Practitioner Candace Craven was sentenced to serve three months in home confinement.

Castro and Syto recruited fellow Marines to receive expensive compounded drugs. Craven and others wrote bogus prescriptions and filled out fraudulent paperwork to process the insurance reimbursements. All told, tens of millions of dollars in false claims were submitted; everyone got kickbacks.

For young Marines this money significantly augmented their monthly paycheck. One defendant noted "it took very little work to sign people up to receive free money."

For recruiting bogus patients, Castro and Syto were paid a commission somewhere between 3 to7 percent of the total TRICARE reimbursement paid to the pharmacy for the drugs sent to their recruits. By the time this fraud scheme was in full swing, the average cost for these compounded drugs was more than $13,000 for a 30-day supply, peaking at around $25,000 for certain individual drugs. Over the course of the conspiracy, the illegal kickbacks amounted to at least $1,013,450.36 for Castro and $264,000 for Syto.

All of the defendants were working for Jimmy and Ashley Collins, a married couple living in Birchwood, Tennessee, who quarterbacked the scheme. Jimmy Collins received a 10-year prison sentence; Ashley Collins was sentenced to 18 months in home confinement. To account for all the fraud, the couple was ordered to pay $65,679,512.71 in restitution to Defense Health Agency and TRICARE.

During the course of the investigation, authorities seized numerous items and properties purchased by the Collinses and others with the proceeds of the fraud: an 82-foot yacht; multiple luxury vehicles, including two Aston Martins; a multimillion-dollar investment annuity; gold and silver bars; dozens of pieces of farm equipment and tractor-trailer trucks; and three pieces of Tennessee real estate. (Source)

Hotel Manager Sentenced To Prison For Paying $103,000+ In Bribes To U.S. Army Training Center Manager - January 29, 2024

On May 3, 2023, a federal grand jury returned a twelve-count Indictment against Alfred Palma and Candy Hanza.

Palma was a United States Army employee and the Manager of the Institutional Training Directed Lodging and Meals (ITDLM) program at Fort Sill, Oklahoma. Palma booked hotel rooms for soldiers who attended off-post trainings. Hanza worked as the general manager of a local hotel. The Indictment alleges that Hanza paid Palma bribes to direct soldiers to Hanza's hotel.

In July 2023, Palma and Hanza pleaded guilty to the bribery scheme. Palma pleaded guilty to receiving bribes totaling $103,200.00 from Hanza in return for favoring the hotel at which Hanza worked as General Manager.

Palma further admitted that he used the cash bribes to purchase money orders from Walmart, which he later deposited into his personal checking account, along with the checks that Hanza gave him. Hanza pleaded guilty to paying a bribe to Palma as a public official. (Source)

U.S. Army Soldier Sentenced To Prison For Role In Drug Trafficking And $700,000+ In Money Laundering - January 26, 2024

On May 7, 2021, U.S. Homeland Security Investigations was notified by the French Customs Service stationed at Charles De Gaulle International airport that a package from Cameroon had been intercepted containing approximately three kilograms of ketamine. The package was delivered to Gordon Ray Custis, then a soldier at Fort Liberty, at his home in Fayetteville, by Federal Task Force Officers with the Cumberland County Sheriff's Office.

Custis pled guilty to possession with the intent to distribute ketamine and he was released pending sentencing. While awaiting sentencing, the Army Criminal Investigative Division and Defense Criminal Investigative Service received information that Custis was laundering money. The subsequent investigation revealed that Custis, acting in a leadership role involving co-defendant and others, laundered over $700,000.

On February 1, 2023, a second search warrant was executed at Custis's home and investigators recovered 28.5 kilograms of ketamine, $164,200 in cash, digital scales and vacuums sealing materials. (Source)

U.S. Army Maintenance Worker Pleads Guilty To Using Fuel Credit Card To Make $33,000+ Of Un-Authorized Fuel Purchases - November 14, 2023

Normas Dais was employed by the United States Army as a civilian maintenance worker at the Fort Lesley J. McNair Department of Public Works.

Dais repeatedly purchased gasoline for private vehicles using a General Services Administration fuel credit card meant solely for a designated maintenance van on the Fort McNair grounds. Investigators found that from April to October of 2023, Dais frequently arranged to meet private vehicles at area gas stations and used his General Services Administration credit card to purchase their gas. In total, Dais made more than 400 unauthorized purchases totaling at least $33,868.21. As part of the plea agreement, Dais agreed to pay full restitution. (Source)

U.S. Navy IT Manager Sentenced To Prison For Hacking A Computer Database, Stealing 9,000 People's Identities & Selling Information For $160,000 In Bitcoin - October 16, 2023

Marquis Hooper is a former Navy IT Manager.

In August 2018, Hooper opened an online account with a company that runs a database containing the PII for millions of people. The company restricts access to the database to businesses and government agencies that have a demonstrated, lawful need for the PII. Hooper, however, opened his database account by falsely representing to the company that the Navy needed him to perform background checks.

After Hooper opened his database account, he added his wife and co-defendant, Natasha Chalk, to the account. They then stole over 9,000 people's PII and sold it to other individuals on the dark web for $160,000 in bitcoin. At least some of the individuals to whom Hooper and Chalk sold the PII used it to commit further crimes.

In December 2018, Hooper's database account was closed for suspected fraud. Thereafter, Hooper, Chalk, and an unindicted co-conspirator tried to regain access to the database. Hooper instructed the unindicted co-conspirator to open a new database account by representing that the Navy needed him to perform background checks just like Hooper had done. Hooper offered to pay the unindicted co-conspirator $2,500 for each month that the database account was opened. The unindicted co-conspirator submitted an application to open the database account and the company told him that a supply officer had to sign the contract.

Hooper then sent the unindicted co-conspirator multiple documents falsely identifying an identity theft victim as the supposed Naval supply officer. These documents included a false contract, a fake driver's license for the identity theft victim, and a forged letter purporting to be from a commanding officer in the Navy. The unindicted co-conspirator submitted the fake documents to the company, but the company decided not to open the new database account. (Source)

U.S. Army Reservist Pleads Guilty For Role In Stealing $101,000+ Of Government Funds - October 13, 2023

Starting in January 2013, and continuing until in or about August 2016, Christopher O'Connor and co-conspirators conspired to obtain money from the Army States under false pretenses by submitting false applications to the Army for military funeral honors (MFH) payment requests for services that had not been performed.

O'Connor proposed submitting false MFH pay requests in the co-conspirators' names in exchange for each sharing their proceeds with O'Connor. In addition to receiving a split of the fraudulent MFH payments from the co-conspirators, O'Connor also submitted and received approximately $18,825.83 in fraudulent MFH payment requests for himself. As a result of this conspiracy, the United States government was defrauded out of approximately $101,858.19.

The National Defense Authorization Act of 2000 authorizes MFH for active-duty soldiers, retirees, and veterans. At a family's request, eligible persons can receive military funeral honors, including the folding and presenting of the United States flag and the playing of Taps. (Source)

U.S. Army Reservist Pleads Guilty To Stealing $15,000 Of Government Funds - August 23, 2023
United States Army Reservist Derrick Branch pled guilty to conspiracy to commit theft of government funds

Branch stole $15,469.30 from the United States Department of the Army by claiming reimbursement for the performance of military funeral honors ceremonies that never happened. (Source)

U.S. Army Reservist Sentenced To Prison For Stealing $21,000+ Of Government Funds - June 16, 2023
Lynea Sanders is a former United States Army Reservist.

Sanders pled guilty to conspiracy to commit theft of government funds, having stolen $21,780.18 from the United States Department of the Army by claiming reimbursement for the performance of military funeral honors ceremonies that never happened. (Source)

U.S. Army Reservist Sentenced To Prison For Stealing $8,300+ Of Government Funds - June 16, 2023
Chantelle Davis is a former United States Army Reservist.

Davis pled guilty to conspiracy to commit theft of government funds, having stolen $8,399.65 from the United States Department of the Army by claiming reimbursement for the performance of military funeral honors ceremonies that never happened. (Source)

U.S. Army Employee Arrested For Accepting $400,000 In Bribery And Kickback Scheme Involving Defense Contracts - May 15, 2023
Young Kim while acting in his capacity as Chief of the Design Branch (2017-2021) at Army Garrison Yongsan / Casey in Korea (USAG-Y/C), developed a scheme to enrich himself through bribes and kickbacks from various manufacturers and suppliers of parts used in U.S. Army contracts.

While acting in that capacity, Kim helped ensure that certain Army contracts included the use of parts manufactured or supplied by specific companies. Some of these parts included blast doors, blast valves, shock mounts, and shock isolators (Equipment Designed To Protect Army Personnel In The Event Of An Attack). In return, the companies manufacturing or supplying those parts collectively sent over $400,000 in kickbacks to Kim. A significant portion of these funds were laundered through bank accounts controlled by Kim's adult relatives, including one account held in the name of a shell company and were ultimately used to enrich Kim and to pay for bills and expenses incurred by Kim. (Source)

U.S. Army Employee Charged For Theft Of $800,000+ Of Military Heavy Equipment - May 10, 2023

From a time unknown but no earlier than November 1, 2021, and continuing through approximately December 31, 2021, Tamilo Fe'a stole military heavy equipment, including vehicles, semi-trailers, generator trailers, flatbed trailers, refrigerator trailers, armored office trailers, tractors, and box vans from the Hawthorne Army Weapons Depot in Hawthorne, Nevada.

The total value of the stolen property was over $800,000.00. From September 2020 to August 2021, Fe'a made about 69 transactions with a fuel fleet credit card for his personal benefit at various gas stations in Nevada, Arizona, New Mexico, and California. (Source)

U.S. Army Contracting Officer For Department of Defense Pleads Guilty In Conspiracy To Defraud The Government Of $490,000 / Used Funds For 31 Vacations - April 24, 2023

Thomas Bouchard was the Contracting Officer in charge of the U.S. Army Natick Contracting Division, a full-service contracting organization for the Department of Defense.

In 2014, Bouchard used his long-standing relationship with Evolution Enterprise, Inc., a government contractor, to allegedly have Chantelle Boyd hired for a "no show" job as an assistant that specifically supported Bouchard. Boyd's position cost the Department of Defense more than $490,000 during her time at Evolution from 2014 to 2018, during which Boyd performed little if any useful function.

Bouchard and Boyd took numerous government-funded trips, ranging in duration from two to 15 days, under the guise that they were work related. This included 31 trips to Orlando, Fla., among other locations such as Clearwater Beach, Fla., and Stafford, Va., during which Boyd allegedly performed little if any work. For many of the trips, Bouchard and Boyd stayed in the same hotel room and spent time at the pool and Disney parks – all during business hours. In order to conceal the personal nature of the trips, Bouchard altered, created and approved false travel to reimburse the Boyd for out-of-pocket expenses. (Source)

2 U.S. Army Officers (Husband, Wife) Plead Guilty To Theft Of Government Property Theft That Profited Them $2 Million+ - April 21, 2023

2 Army Officers (Husband, Wife) have been convicted in a multi-year activity involving the theft of more than $2 Million in government property. Chief Warrant Officer Three (CW3) Christopher Hammond pled guilty to theft / possession of government property and money laundering. His wife Major Heather Hammond was convicted for spending money laundering proceeds and aiding and abetting.

CW3 Hammond used his position to requisition government property intended for his unit at Ft. Bragg. The property was never logged into inventory at the base but was instead sold by Hammond to various individuals. In a two-year period, CW3 Hammond received at least $1.8 million in wire transfers related to the sales, which he deposited into bank accounts controlled by him and his wife. The investigation traced about 200 items sold by CW3 Hammond or held in his home as having been issued to Hammond's military unit.

Major Hammond knowingly allowed use of her bank accounts, even suggesting the use of her accounts so the money would not go into Chief Hammond's bank account. The fraud was uncovered when a supplier noticed that items procured under a government contract were being sent in for warranty repairs by a private individual. (Source)

U.S. Navy Doctor Pleads Guilty To Role In Defrauding The Navy Of $2 Million / Received $180,000 In Kickbacks - March 28, 2023

Dr. Michael Villarroel, a U.S. Navy Doctor, pleaded guilty in federal court, admitting that he and others conspired to defraud the Navy by faking or exaggerating injuries to obtain insurance payments intended to help service members recovering from traumatic injuries. Villarroel acknowledged he knew the claimed injuries were false or exaggerated but signed off on applications for a share of the insurance payments.

Villarroel admitted that from 2012 to at least December 2015, he conspired to commit wire fraud with Christopher Toups, a Chief Petty Officer Construction Mechanic in the Navy; Kelene Meyer, Toups' spouse and a nurse; and others. Toups prodded other service members to submit claims, told them to provide medical records to Meyer, requested part of the insurance payment in return, and distributed shares to Meyer and Villarroel. Meyer used her medical background to falsify or doctor supporting records to reflect fake or exaggerated injuries.

Participants in the scheme obtained about $2 Million in payments from the Traumatic Service members Groups Life Insurance (TSGLI) program which is funded by service members and the Navy. Villarroel personally obtained more than $180,000 in kickbacks. (Source)

U.S. Army Solider Sentenced To Prison For Role In $3.5 Million+ COVID-19 Fraud Scheme - January 9, 2023

Dara Buck, a U.S. Army Chief Warrant Officer, stationed at Fort Stewart, has been sentenced to federal prison for leading a prolific fraud scheme in which she and others illegally raked in millions of dollars from COVID-19 relief programs and federal student loan forgiveness.

From August 2017 through May 2021, Buck led a conspiracy to fraudulently obtain funding from the Coronavirus Aid, Relief, and Economic Security (CARES) Act's Paycheck Protection Program (PPP), and to secure the fraudulent discharge of federal student loans using falsified disability claims.

Buck admitted submitting more than 150 fraudulent PPP loan applications to the Small Business Administrating for herself and others in the conspiracy, resulting in more than $3 million in fraudulent disbursements from banks to members of the conspiracy. Buck directly received fraudulently obtained PPP funding, or was paid by conspirators for submitting their fraudulent applications.

In addition, conspirators paid Buck to submit falsified U.S. Department of Veterans Affairs certifications for total and permanent disability to the U.S. Department of Education in order to fraudulently secure the discharge of more than a dozen student loans totaling more than $1 million. (Source)

4 U.S. Army Depot Officials & Vendors Sentenced To Prison For $7 Million+ Contracting & Bribery Scheme - September 13, 2022

Jimmy Scarbrough was the Equipment Mechanic Supervisor at the Red River Army Depot (RRAD) in Texarkana, Texas, a position he held from November 2001 until May 2019.

Scarbrough directed more than $7 million in purchases from RRAD to RRAD Vendor Jeffrey Harrison and Justin Bishop through the government purchase card (GPC) program. In order to manipulate the GPC program, which is designed to ensure a competitive bidding process, Scarbrough told the vendors what to bid, including the item, the quantity, and the price. By collecting fake bids from multiple vendors, Scarbrough was able to direct RRAD purchases to his select vendors, in this case Harrison and Bishop, while maintaining the appearance of a competitive bidding process.

Scarbrough also defrauded the United States by falsely certifying that he had received the purchased items, therefore causing the RRAD to pay his select vendors. However, the reality was that Scarborough instructed the vendors not to deliver certain RRAD-purchased items.

Scarbrough demanded hundreds of thousands of dollars in bribes from his selected vendors. Scarbrough accepted bribes in various forms, including receiving at least $116,000.00 in U.S. Postal Service money orders from Harrison.

Scarbrough also had Harrison and Bishop purchase at least $135,000.00 in car parts or services for his hot rod collection, which included a red and black 1936 Ford Tudor, an electric green 1932 Ford Coupe, a cherry red 1951 Ford F-1 truck, and more. Scarbrough received more than $27,000.00 worth of firearms from Bishop, including rare Colt handguns and Wurfflein dueling pistols. Finally, Scarbrough directed at least $32,000.00 in donations to the Hooks Volunteer Fire Department while he was the Capitan of Operations. In total, Scarbrough received more than $300,000.00 in bribe payments from Harrison and Bishop.

Scarbrough is not the only official at RRAD who accepted bribes. Devin McEwin accepted more than $21,000.00 in bribes from Harrison, including hunting trips, donations directed to the Annona Volunteer Fire Department, and the refurbishment of his 1964 Ford truck. Additionally, Louis Singleton accepted more than $18,000 in bribes from Harrison and others, including tickets to the Hall of Fame section of AT&T Stadium for the Dallas Cowboys football game against the New England Patriots. Singleton was the supervisor of the GPC program at the RRAD and was responsible for approving purchases requested by Scarbrough. (Source)

Construction Company CEO Admits To Paying $95,000+ In Bribes To U.S. Army Biochemist Researcher For $1 Million+ In Government Contracts - February 25, 2022

John Conigliaro is the owner and Chief Executive Officer of EISCO, Inc. EISCO provides general construction services, including fixed and portable biochemical laboratories.

From 2012 to 2019, Conigliaro bribed an Army Research Biologist, who worked at the U.S. Army Combat Capabilities Development Command (CCDC) Chemical Biological Center (CB Center), located on Aberdeen Proving Ground, in Maryland.

Conigliaro provided the Army Research Biologist with a stream of benefits including cash loans, payments for renovations to rental properties, payments for renovations to his personal residence, and other things of value in exchange for influencing CB Center projects to EISCO.

In October 2013, after EISCO received its first payment of $150,000 for a government project, Conigliaro gave cash and a $40,000 zero-interest loan to the Army Research Biologist to finance the purchase of two rental properties. Conigliaro paid for thousands of dollars of renovations to the rental properties.

Additionally, from 2016 to 2018, the Army Research Biologist directed three CB Center projects to EISCO. During the performance of one of those projects, Conigliaro spent approximately half of the time not performing work but being "on call." Conigliaro paid for more than $30,000 in renovations to his personal residence, including more than more than $20,000 to renovate the kitchen, and more than $16,000 to replace the siding on his personal residence.

From July 2012 to 2019, Conigliaro paid more than $95,000 in bribes to the Army Research Biologist, and over that same time period, Army Research Biologist directed more than $1 million of contract awards to EISCO. (Source)

Former U.S. Army Employee Sentenced To Prison For Kickback Scheme To Steer $3 Million+ Of U.S. Government Contracts To Specific Company - November 10, 2021

Ephraim Garcia is a former civilian employee of the U.S. Army's Directorate of Public Works. He was sentenced to two years in prison for a kickback scheme to steer government contracts for work at Camp Arifjan, a U.S. Army base in Kuwait.

Garcia admitted that he conspired with Gandhiraj Sankaralingam, the former general manager and co-owner of Kuwait-based contracting company Gulf Link Venture Co. W.L.L. (Gulf Link), to steer government contracts to Gulf Link.

In his position with the U.S. Army, Garcia was involved in the solicitation, award and management of certain government contracts related to facilities support at Camp Arifjan.

In 2015, at an Olive Garden restaurant located in Mahboula, Kuwait, Garcia and Sankaralingam approached an employee of the prime contractor responsible for base support services.

During that meeting, they offered to pay the prime-contractor employee in exchange for his assistance in steering subcontracts worth over $3 million to Gulf Link. Rather than agree to the scheme, the prime-contractor employee reported the kickback offer to authorities. (Source)

U.S. Army National Guardsman And DoD Subcontractor Charged With Conspiring To Steal / Sell Military Gear And Uniforms - August 19, 2021

Brandon Schulte, Jody Stambaugh and Gary Stambaugh, are accused of conspiring with each other and others unnamed to steal military uniforms, tactical robots, night vision sights, high frequency radios, and other functional military equipment.

Jody Stambaugh and Joe Stambaugh were co-owners of Stambaugh Enterprises, a scrap metal company. Stambaugh Enterprises allegedly operated as a subcontractor on a DoD contract to pick-up, transport, and recycle scrap metal items from multiple DoD facilities in Illinois and Missouri, including Scott Air Force Base in St. Clair County, Illinois, and a Missouri Army National Guard facility in Jefferson City, Missouri.

The Stambaughs were obligated to mutilate and destroy all military property they hauled away from each DoD facility and were prohibited from reusing or refurbishing any military items for their own use or selling any military items to be reused or refurbished by someone else.

The Stambaughs allegedly removed truckloads of military property from DoD facilities but did not destroy or mutilate every item, in violation of their contracts. The Stambaughs transported the military property to their place of business in Mascoutah and sorted through the items to determine what could be converted to their own use or sold to others.

Brandon Schulte was a National Guardsman responsible for properly storing and disposing of military property at the Missouri Army National Guard facility in Jefferson City. The Stambaughs received military uniforms and other unauthorized, sensitive military property from Schulte, even though Schulte allegedly knew the Stambaughs were authorized to receive only scrap metal.

The indictment charges that Schulte understood he was required to follow specific procedures to dispose of sensitive military items, including uniforms.

Such procedures are vital to national security, as terrorist groups overseas have previously acquired U.S. combat uniforms and used them to impersonate American soldiers, endangering American troops. Nevertheless, Schulte allegedly supplied the Stambaughs with thousands of pounds of military uniforms and other non-scrap military equipment. (Source)

U.S Navy 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 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, 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 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)

U.S. Navy Contracting Official Pleads Guilty To Taking $37,000 In Cash Bribes To Aid Contractor's Request For $6.4 Million From DoD - July 13, 2021

In 2014 and 2015 Nizar Farhat was on assigned temporary duty at the United States Navy Base Camp Lemonnier in Djibouti, Africa where he oversaw a private company's $15 million contract to construct an aircraft hangar and a telecommunications facility. After the projects were completed, the company submitted to the Defense Department Requests for Equitable Adjustment (REA) that sought $6.43 million in additional payments.

Farhat admitted that, on four separate occasions between December 2015 and October 2017, he met with representatives of the contracting company at hotels in Las Vegas and Palm Springs. During those meetings, Farhat took $15,000 in cash to help draft the REA the company submitted to the DoD, and another $22,000 in cash to recommend that the Navy certify completion of the construction projects and approve the REA. Following those meetings, Farhat urged the DoD to approve the majority of the REAs, without disclosing that defendant had received cash from the company in exchange for his recommendation. (Source)

U.S. Marine Sentenced To Prison For Illegal Exportation Of Firearms And Controlled Equipment To Haitian Army - March 2, 2021

On December 12, 2020, Jacques Duroseau was convicted of conspiracy to illegally export and smuggle firearms and controlled equipment from the United States to Haiti, as well as transporting firearms without a license to the Haitian Army.

At trial, the evidence showed that Duroseau, at the time an active duty U.S. Marine with the rank of sergeant, along with a co-conspirator, both impersonated high ranking military officers and pretended to be on military business in order to facilitate the illegal transportation of eight firearms, including a Ruger model Precision Rifle 300WIN MAG and a Spike's Tactical model ST15, as well as copious ammunition, riflescopes, and body armor, via commercial aircraft to Haiti. The evidence further showed that Duroseau's purpose was to train the Haitian Army with the firearms and equipment in order to engage in foreign armed conflict. (Source)

Government Contractor Sentenced To Prison For Paying $100,000+ In Bribes To 2 U.S. Army Contracting Officials For $19 Million Worth Of Contracts - January 15, 2021

John Winslett admitted that from 2011 to 2018, he paid over $100,000 worth of bribes to two U.S. Army contracting officials who worked at the Range at Schofield Barracks, in order to steer federal contracts worth at least $19 million to his employer, a government contractor. The bribes included cash, automobiles, and firearms. In return, the contracting officials used their positions to benefit Winslett's employer in securing U.S. Army contracts. (Source)

2 U.S. Army Reservists Plead Guilty For Involvement In $3 Million+ Fraud And Money Laundering Scheme - December 23, 2020

From February 2018 through at September 2019, Joseph Asan and Charles Ogozy were members of the U.S. Army Reserves who participated in a scheme to commit fraud against victims across the United States, defraud banks, and launder over $3 million in fraud proceeds in bank accounts that they controlled.

The funds laundered by Asan and Ogozy were obtained primarily through (a) business email compromises, in which members of the scheme gained unauthorized access to or spoofed email accounts and impersonated employees of a company or third parties engaged in business with the company in order to fraudulently induce the victims to transfer money to bank accounts under the control of members of the scheme; and (b) romance scams, in which members of the scheme deluded unsuspecting older women and men into believing they were in a romantic relationship with a fake identity assumed by members of the scheme and used false pretenses to cause the victims to transfer money to bank accounts under the control of members of the scheme, including Asan and Ogozy. Notably, one of the victims of the defendants' scheme included a U.S. Marine Corps veteran's organization.

In order to launder over $3 million in proceeds from those fraud schemes, Asan and Ogozy opened several bank accounts in the names of fake businesses called Uxbridge Capital LLC, Renegade Logistics LLC, and Eldadoc Consulting LLC and received fraud proceeds in those bank accounts. Asan and Ogozy then laundered the fraud proceeds to each other and to other co-conspirators based in Nigeria. (Source)

U.S Government Employee And U.S. Army National Guardsman Sentenced To Prison For Stealing And Selling $2.4 Million+ Worth Of Sensitive U.S. Military Equipment - November 19, 2020

A judge sentenced a former U.S. Property and Fiscal Office Program Analyst (Joseph Mora) and a former Texas Army National Guardsman (Cristal Avila) to prison for selling on the internet over $2.4 million in sensitive military equipment stolen from Camp Mabry in Austin, Texas.

According to court records, from 2016 to 2019, Mora and Avila stole large quantities of government property, including scopes, infrared laser aiming devices and thermal night vision goggles, with an estimated value in excess of $2.4 million. Mora and Avila later sold the stolen goods on eBay and elsewhere. (Source)

Oregon National Guard Employee Sentenced To Prison For Role In $6 Million Government Contracting Fraud Scheme - November 2, 2020

From approximately 2009 through 2014, Dominic Caputo served as the Program Manager of the Power Division of the Oregon National Guard's OSMS at Camp Withycombe, an Oregon Military Department installation. OSMS supports readiness and training of the U.S. Military by refurbishing out-of-service electronic equipment owned by the DoD. In the event of an emergency or declaration of war, OSMS deploys refurbished equipment to other military bases or installations.

During the time alleged in the Indictment and until 2015, OSMS was the only maintenance site in the United States capable of repairing and rebuilding certain models of electric generators and other small engines and parts in support of the federal military supply system.

In Fiscal Year 2014, Caputo billed the U.S. Army's Communications-Electronics Command (CECOM) more than $675,000 for the repair and rebuilding of John Deere Diesel Engines despite the work having not been performed. More than 60 of the engines had already been repaired and billed to CECOM in prior fiscal years. For those engines, Caputo directed Power Division employees to remove and replace original serial numbers and identifying engine plates from the engines to conceal the duplicate billing.

In June 2014, Caputo willingly and knowingly prepared a work order and run test data indicating that the falsified repair work on an engine had been performed. Caputo submitted this false information to CECOM.

Caputo's employment with OSMS was terminated in November 2014 when his fraud was revealed. Caputo billed for $6 million in repairs that were never done. (Source)

U.S. Navy Chief Petty Officer Sentenced To Prison For Bribery Conspiracy With Foreign Defense Contractor Involving 50+ Individuals - October 30, 2020

Brooks Parks, a U.S. Navy Chief Petty Officer, is that latest to be sentenced in the wide-ranging corruption and fraud investigation involving foreign defense contractor Leonard Francis and his Singapore-based company, Glenn Defense Marine Asia (GDMA).

Francis pleaded guilty in 2015 to bribery and fraud charges, admitting that he presided over a massive, decade-long conspiracy involving scores of U.S. Navy officials, tens of millions of dollars in fraud and millions of dollars in bribes - from cash, prostitutes and luxury travel accommodations to Cuban cigars, Kobe beef and Spanish suckling pigs.

So far, 34 defendants have been charged and 23 have pleaded guilty as part of this investigation, many admitting they accepted luxury travel and accommodations, meals or services of prostitutes from Francis in exchange for helping GDMA win and maintain contracts and over bill the Navy by millions of dollars.

From December 2005 to February 2009 Parks served as the Logistics Lead Petty Officer on the USS Blue Ridge, the command ship for the Seventh Fleet. Parks was actively involved in managing the Seventh Fleet's logistics support budget, signing and processing invoices, and performing other supervisory logistics functions for the Seventh Fleet.

Parks admitted that from March 2006 through March 2010, Francis paid for lavish hotel accommodations for Parks and his friends throughout Asia, as the USS Blue Ridge came into port. Parks had expensive taste and wasn't restrained in demanding ever more luxuriant accommodations from GDMA. In one instance, Parks demanded the $4,800 per night Ritz Carlton Suite in Singapore, though he was ultimately provided

In return for these bribes, Parks approved and expedited GDMA invoices and payment requests, provided substantial bidding and pricing information to GDMA as part of GDMA's effort to crush its competitor in the Philippines, and provided limited ship port visit scheduling information. (Source)

U.S. Navy Warehouse Manager Who Stole And Sold $2.5 Million Worth Of Military Goods Sentenced To Prison - August 24, 2020

Herbert Gutierrez, is a former warehouse manager at the U.S. Navy Military Sealift Command (MSC) Warehouse in San Diego, and a 20-year veteran of the U.S. Navy. He was sentenced to prison for stealing more than $2.5 million worth of goods from the Navy warehouse where he worked.

Gutierrez began stealing from the warehouse for his own personal gain a few months after he started working there. For approximately nine months, between July 2018 and April 2019, Gutierrez advertised items from the warehouse for sale online, including through such websites as eBay, and then allowed private individuals into the MSC warehouse yard during work hours and after hours to take the government property, load it onto trucks, and haul it away. (Source)

And Many More…….

PREVIOUS INSIDER THREAT INCIDENTS REPORTS
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

DOD FRAUD RESOURCES

In the private sector fraud is also a big problem.

The 2024 Association of Certified Fraud Examiners is based on 1,921 real cases of occupational fraud, includes data from 138 countries and territories, covers 22 major industries and explores the costs, schemes, victims and perpetrators of fraud. These fraud cases caused losses of more than **$3.1 BILLION**. (Download Report)

This report states that more than half of frauds occurred **due to lack of internal controls or an override of existing internal controls.**

The report also states that providing fraud awareness training to staff at all levels of an organization is a vital part of a comprehensive anti-fraud program. The report states that training employees, managers, and executives about the risks and costs of fraud, can help reduce fraud losses and ensure frauds are caught more quickly. **43% of frauds were detected by a tip**.

DOD FRAUD DETECTION RESOURCES

General Fraud Indicators & Management Related Fraud Indicators

Fraud Red Flags & Indicators

Comprehensive List Of Fraud Indicators

Insider Threat Detection Tool (ITDT) Capabilities - Identifying Gaps, Defining Requirements

A 2018 DoD PERSERC Report Titled: A Strategic Plan To Leverage The Social & Behavioral Sciences To Counter The Insider Threat, Stated The Following:
"UAM and UEBA tools are expensive, and critics have begun to ask whether the value-add sufficiently exceeds the price tag, especially when these tools have steep learning curves. According to several SMEs, many tools were not designed with end-users in mind, cannot be quickly deployed “out of the box”, and / or require maintenance that causes lengthy outages. In the absence of comprehensive and free market surveys, consumers have begun to educate themselves on open source solutions that could meet their needs without the corresponding high cost.

Beyond which tool to purchase is the question of what types of data exist and of those, which provide the most insight into insider threat behavior." (Source)

It is now 2024. Research conducted among NITSIG members shows a continued concern that some organizations purchase an ITDT based of vendor sales pitches, flashy demos and from primarily an IT / data centric perspective.

Defining the organizations requirements for an ITDT is critical to protecting the organizations assets which comprise Facilities, Employees, Financial Assets, Data, Computer Systems and Networks.

BEHAVIORAL INDICATORS OF CONCERNS

Lack of communications between departments / stakeholders with the ITP, is a common problem that leads to the failure to identify employees who may pose risks or serious threats to an organization.

To identify a potential or actual Insider Threat concern requires looking at numerous sources of information (Non-Technical, Technical) to create an accurate risk / threat profile of an employee.

Various departments or stakeholders supporting the ITP (Supervisors, Security, Human Resources, IT, Employees, Etc.) may have the individual nuggets / information that will substantiate or refute the risks or threats an employee may pose to the organization.

The documents listed below are excellent educational resources to share with stakeholders supporting the ITP. The better educated stakeholders are at recognizing and reporting behavioral indicators of concern, the better chance the organization has of being proactive in identifying risks and threats to the organization by employees.

Behavioral Indicators Of Concern For Insider Threat Programs Part 1

Behavioral Indicators Of Concern For Insider Threat Programs Part 2

DCSA Insider Threat Potential Risk Indicators Guide

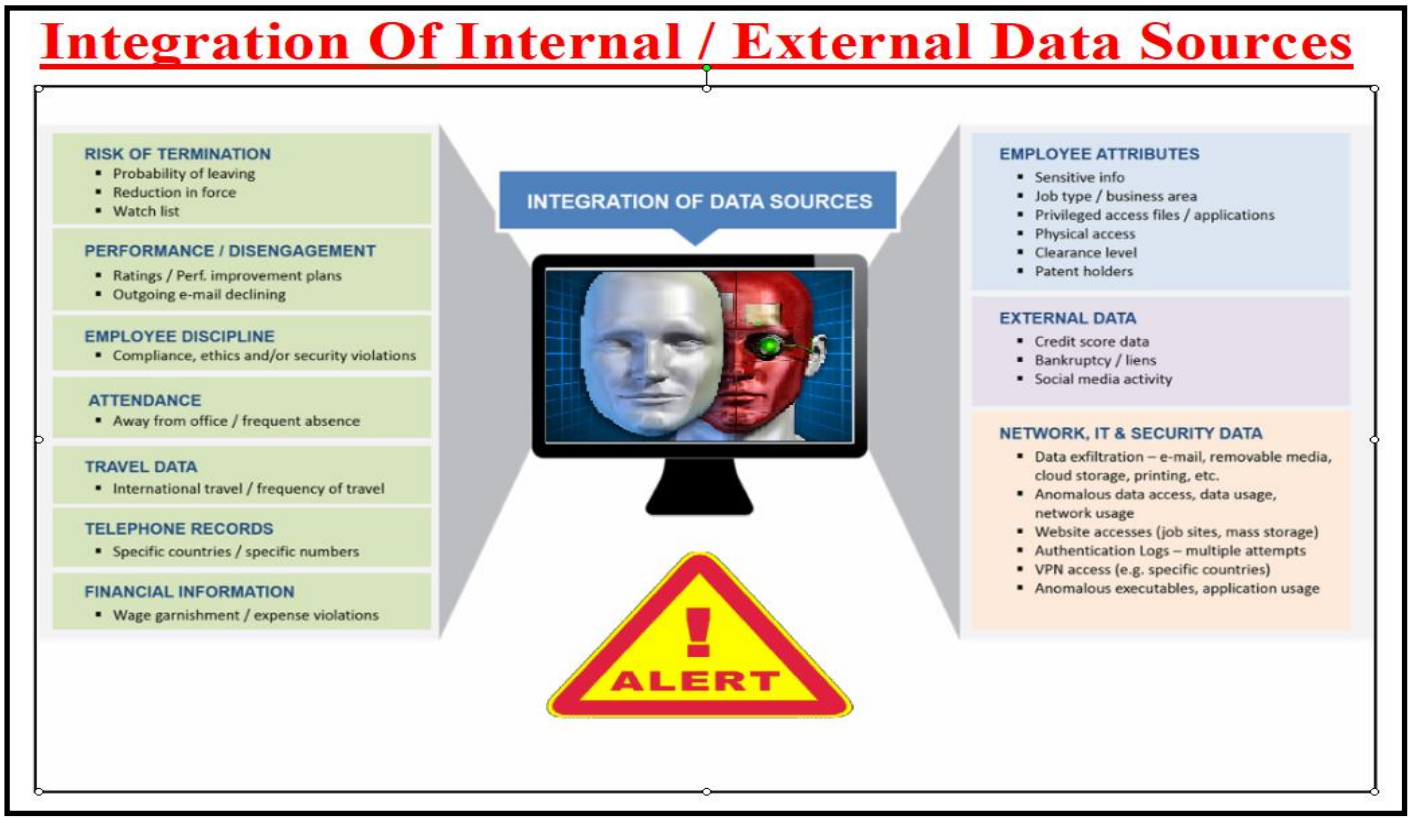
DCSA Roles & Responsibilities For Personnel Security - A Guide For Supervisors

DCSA Insider Threat Behavioral Indicators Brochure

Application Of The Critical-Path Method To Evaluate Insider Risks

Using External Data Sources For Insider Threat Detection & Mitigation

A Guide For Employers To Implement A Continuous Screening Program



DEFINITIONS OF INSIDER THREATS

The following pages are related to Insider Threats in the private sector, and aim to provide a holistic view of the problem, beyond the DoD.

The definition of Insider Threats can be vast, and must go beyond current definitions (By Sources Such As: National Insider Threat Policy, NISPOM Conforming Change 2 & 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
- ☐ Damage Or Theft Of Organizations Assets (Physical, Etc.)
- ☐ 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, Fake Shell Companies / Fake Invoice Schemes
- ☐ Employees' Involved In Bribery, Kickbacks, Blackmail, Extortion
- ☐ Data, Computer & Network Sabotage / Misuse
- ☐ Employees' Working Remotely Holding 2 Jobs In Violation Of Company Policy
- ☐ 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
- ☐ Geopolitical Risks (Employee Loyalty To Company Vs. Country Because Of U.S. - Foreign Nation Conflicts)

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 (Pilots, Flight Attendants, Etc.)
  - 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, Etc.)
- ☐ 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 / Lawsuits
- ☐ Employees' Lose Jobs / Company Goes Out Of Business

DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)

- ☐ Negative Performance Review, No Promotion, No Salary Increase, No Bonus
- ☐ Transferred To Another Department / Un-Happy
- ☐ Demotion, Sanctions, Reprimands Or Probation Imposed Because Of Security Violation Or Other Problems
- ☐ Not Recognized For Achievements
- ☐ Lack Of Training For Career Growth / Advancement
- ☐ Failure To Offer Severance Package / Extend Health Coverage During Separations – Terminations
- ☐ Reduction In Force, Merger / Acquisition (Fear Of Losing Job)
- ☐ Workplace Violence As A Result Of Being Terminated

MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST

- ☐ The Company Owes Me Attitude (Financial Theft, Embezzlement)
- ☐ Need Money To Support Gambling Problems / Payoff Debt, Personal Enrichment For Lavish Lifestyle

IDEOLOGY

- ☐ Opinions, Beliefs Conflict With Employer, Employees', U.S. Government (Espionage, Terrorism)

COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Bribery, Extortion, Blackmail

COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Persuading Employee To Contribute In Malicious Actions Against Employer (Insider Threat Collusion)

OTHER

- ☐ New Hire Unhappy With Position
- ☐ Supervisor / Co-Worker Conflicts
- ☐ Work / Project / Task Requirements (Hours Worked, Stress, Unrealistic Deadlines, Milestones)
- ☐ Or Whatever The Employee Feels The Employer Has Done Wrong To Them

NITSIG research indicates many employees may not be disgruntled, but have other motives such as financial gain to live a better lifestyle, etc.

You might be shocked as to what employees do with the money they steal or embezzle from organizations and businesses, and how many years they got away with it, until they were caught. (1 To 20 Years)

What Do Employees' Do With The Money They Embezzle / Steal From Federal / State Government Agencies & Businesses Or With The Money They Receive From Bribes / Kickbacks?

They Have Purchased:
Vehicles, Collectible Cars, Motorcycles, Jets, Boats, Yachts, Jewelry, Properties & Businesses

They Have Used Company Funds / Credit Cards To Pay For:
Rent / Leasing Apartments, Furniture, Monthly Vehicle Payments, Credit Card Bills / Lines Of Credit, Child Support, Student Loans, Fine Dining, Wedding, Anniversary Parties, Cosmetic Surgery, Designer Clothing, Tuition, Travel, Renovate Homes, Auto Repairs, Fund Shopping / Gambling Addictions, Fund Their Side Business / Family Business, Grow Marijuana, Buying Stocks, Firearms, Ammunition & Camping Equipment, Pet Grooming, And More.....

They Have Issued Company Checks To:
Themselves, Family Members, Friends, Boyfriends / Girlfriends

INSIDERS WHO STOLE TRADE SECRETS / RESEARCH FOR CHINA / OR HAD TIES TO CHINA

CTTP = China Thousand Talents Plan

- NIH Reveals That 500+ U.S. Scientist's Are Under Investigation For Being Compromised By China And Other Foreign Powers
- U.S. Petroleum Company Scientist STP For $1 Billion Theft Of Trade Secrets - Was Starting New Job In China
- Cleveland Clinic Doctor Arrested For $3.6 Million Grant Funding Fraud Scheme Involving CTTP
- Hospital Researcher STP For Conspiring To Steal Trade Secrets And Sell Them in China With Help Of Husband
- Employee Of Research Institute Pleads Guilty To Steal Trade Secrets To Sell Them In China
- Raytheon Engineer STP For Exporting Sensitive Military Technology To China
- GE Power & Water Employee Charged With Stealing Turbine Technologies Trade Secrets Using Steganography For Data Exfiltration To Benefit People's Republic of China
- CIA Officer Charged With Espionage Over 10 Years Involving People's Republic of China
- Massachusetts Institute of Technology (MIT) Professor Charged With Grant Fraud Involving CTTP
- Employee At Los Alamos National Laboratory Receives Probation For Making False Statements About Being Employed By CTTP
- Texas A&M University Professor Arrested For Concealing His Association With CTTP
- West Virginia University Professor STP For Fraud And Participation In CTTP
- Harvard University Professor Charged With Receiving Financial Support From CTTP
- Visiting Chinese Professor At University of Texas Pleads Guilty To Lying To FBI About Stealing American Technology
- Researcher Who Worked At Nationwide Children's Hospital's Research Institute For 10 Years, Pleads Guilty To Stealing Scientific Trade Secrets To Sell To China
- U.S. University Researcher Charged With Illegally Using $4.1 Million In U.S. Grant Funds To Develop Scientific Expertise For China
- U.S. University Researcher Charged With VISA Fraud And Concealed Her Membership In Chinese Military
- Chinese Citizen Who Worked For U.S. Company Convicted Of Economic Espionage, Theft Of Trade Secrets To Start New Business In China
- Tennessee University Researcher Who Was Receiving Funding From NASA Arrested For Hiding Affiliation With A Chinese University
- Engineers Found Guilty Of Stealing Micron Secrets For China
- Corning Employee Accused Of Theft Of Trade Secrets To Help Start New Business In China
- Husband And Wife Scientists Working For American Pharmaceutical Company, Plead Guilty To Illegally Importing Potentially Toxic Lab Chemicals And Illegally Forwarding Confidential Vaccine Research to China
- Former Coca-Cola Company Chemist Sentenced To Prison For Stealing Trade Secrets To Setup New Business In China
- Former Scientist Convicted For Role With Sister To Steal Trade Secrets From GlaxoSmithKline Worth $10 BILLION To Setup Business In China
- University Of Kansas Researcher Convicted For Hiding Ties To Chinese Government
- Former Employee (Chinese National) Sentenced To Prison For Conspiring To Steal Trade Secret From U.S. Company
- Federal Indictment Charges People's Republic Of China Telecommunications Company With Conspiring With Former Motorola Solutions Employees' To Steal Technology

- Former U.S. Navy Sailor Sentenced To Prison For Selling Export Controlled Military Equipment To China With Help Of Husband Who Was Also In Navy
- Former Broadcom Engineer Charged With Theft Of Trade Secrets - Provided Them To His New Employer A China Startup Company

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present / Updated Daily

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**5,400+ 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 - WORKPLACE VIOLENCE INCIDENTS E-MAGAZINE

This e-magazine is frequently updated with the workplace violence incidents.

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

https://flipboard.com/@cybercops911/insider-threat-workplace-violence-incidents-e-magazine-r8avhdlcz

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

http://www.insiderthreatincidents.com **or**
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

INSIDER THREAT INCIDENTS SPOTLIGHT REPORT FOR 2023

This comprehensive **EYE OPENING** report provides a **360 DEGREE VIEW** of the many different types of malicious actions employees' have taken against their employers.

This is the only report produced that provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes. (U.S. Government, Private Sector)
https://nationalinsiderthreatsig.org/pdfs/insider-threats-incidents-malicious-employees-spotlight-report%20for%202023.pdf

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

Updated Daily

https://twitter.com/InsiderThreatDG
Follow Us On Twitter: @InsiderThreatDG

National Insider Threat Special Interest Group (NITSIG)

U.S. / Global Insider Risk Management (IRM) Information Sharing & Analysis Center
Educational Center Of Excellence For IRM & Security Professionals

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center, as no such ISAC existed. The NITSIG has been successful in bringing together IRM and other security professionals from the U.S. Government, Department of Defense, Intelligence Community Agencies, universities and private sector businesses, to enhance the collaboration and sharing of information, best practices and resources related to IRM. This has enabled the NITSIG membership to be much more effective in identifying, responding to and mitigating Insider Risks and Threats.

NITSIG Membership

The NITSIG Membership (**Free**) is the largest network (**1000+**) of IRM professionals in the U.S. and globally. Our member's willingness to share information has been the driving force that has made the NITSIG very successful.

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

- ✓ Insider Risk Management Programs (Development, Management & Optimization)
- ✓ Insider Risk Management Program Working Group / Hub Operations
- ✓ Insider Threat Awareness Training
- ✓ Insider Risk / Threat Assessments & Mitigation Strategies
- ✓ Insider Threat Detection Tools (UAM, UBA, DLP, SEIM) (Requirements Analysis & Purchasing Guidance
- ✓ Employee Continuous Monitoring & Reporting Programs
- ✓ Insider Threat Awareness Training
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

NITSIG Meetings

The NITSIG provides education and guidance to the membership via in person meetings, webinars and other events, that is practical, strategic, operational and tactical in nature. Many members have even stated the NITSIG is like having a team of IRM experts at their disposal FREE OF CHARGE. 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

NITSIG IRM Resources

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

NITSIG LinkedIn Group

The NITSIG has created a Linked Group for individuals that are interested in sharing and gaining in-depth knowledge related to IRM and IRM Programs. This group will also enable the NITSIG to share the latest news and upcoming events. We invite you to join the NITSIG LinkedIn Group. You do not have to be a NITSIG member to be join this group: https://www.linkedin.com/groups/12277699

NITSIG Insider Threat Symposium & Expo

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 Insider Threat Program Managers / Insider Risk Program Managers with ***Hands On Experience***.

At the expo are many vendors that showcase their training, services and products. This link provides all the vendors that exhibited at the 2019 ITS&E, and provides a description of their solutions for Insider Threat detection and mitigation.

ITS&E events were not held in 2020 to 2023 because of COVID. The next ITS&E is scheduled for March 4, 2025 at the John Hopkins University Applied Physics Lab in Laurel, Maryland

The ITS&E provides attendees with access to a large network of security professionals for collaborating with on all aspects of IRM.

NITSIG Advisory Board

The NITSIG Advisory Board (AB) is comprised of IRM Subject Matter Experts with extensive experience in IRM Programs. AB members have managed U.S. Government Insider Threat Programs, or currently manage or support industry and academia IRM Programs. Advisory board members will provide oversight and educational / strategic guidance to support the mission of the NITSIG, and also help to facilitate building relationships with individuals that manage or support IRM Programs. The link below provided a summary of AB members' backgrounds and experience in IRM.
https://www.nationalinsiderthreatsig.org/aboutnitsig.html

INSIDER THREAT DEFENSE GROUP

Insider Risk Management Program Experts

Since 2014, the Insider Threat Defense Group (ITDG) has had a long standing reputation of providing our clients with proven experience, past performance and exceptional satisfaction.

The ITDG offers the most affordable, comprehensive and practical training courses and consulting services to help organizations develop, implement, manage and optimize an Insider Risk Management Program.

Over **1000+** individuals have attended our highly sought after Insider Threat Program (ITP) Development, Management & Optimization Training Course (Classroom & Live Web Based) and received ITP Manager Certificates.

The ITDG are experts at providing guidance to help build Insider Threat Programs (For U.S. Government Agencies, Defense Contractors) and Insider Risk Management Programs for Fortune 100 / 500 companies and others. We know what the many internal challenges are that an Insider Risk Program Manager may face. There are many interconnected cross departmental components and complexities that are needed for comprehensive Insider Risk Management. We will provide the training, guidance and resources to ensure that the Insider Risk Program Manager and key stakeholders are universally aligned from an enterprise / holistic perspective to detect and mitigate Insider Risks and Threats.

INSIDER RISK MANAGEMENT (IRM) PROGRAM CONSULTING SERVICES OFFERED

Conducted Via Classroom / Onsite / Web Based

- ✓ Executive Management & Stakeholder Briefings For IRM
- ✓ IRM Program Training & Workshops For C-Suite, Insider Risk Program Manager / Working Group, Insider Threat Analysts & Investigators
- ✓ IRM Program Development, Management & Optimization Training & Related Courses
- ✓ Insider Risk - Threat Vulnerability Assessments
- ✓ IRM Program Maturity Evaluation, Gap Analysis & Strategic Planning Guidance
- ✓ Insider Threat Awareness Training For Employees'
- ✓ Insider Threat Detection Tool Gap Analysis & Pre-Purchasing Guidance / Solutions
- ✓ Data Exfiltration Assessment (Executing The Malicious Insiders Playbook Of Tactics)
- ✓ Technical Surveillance Counter-Measures Inspections (Covert Audio / Video Device Detection)
- ✓ Employee Continuous Monitoring & Reporting Services (External Data Sources)
- ✓ Customized IRM Consulting Services For Our Clients

The ITDG Has Provided IRM Training / Consulting Services To An Impressive List Of Clients:

White House, U.S. Government Agencies, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines), Intelligence Community Agencies (DIA, NSA, NGA), Law Enforcement (DHS, TSA, FBI, U.S. Secret Service, DEA, Police Departments), Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft, Verzion, Walmart, Home Depot, Nike, Tesla, Dell Technologies, Nationwide Insurance, Discovery Channel, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more. The ITDG has provided training and consulting services to over **675+** organizations. (Client Listing)

Additional Background Information On ITDG

Mr. Henderson is the CEO of the ITDG, Founder / Chairman of the NITSIG and Founder / Director of the Insider Threat Symposium & Expo (ITS&E). Combining NITSG meetings, ITS&E events and ITDG training / consulting services, the NITSIG and ITDG have provided IRM Guidance and Training to **3,400+** individuals.

The NSA previously awarded the ITDG a contract for an Information Systems Security Program / IRM Training Course. This course was taught to **100** NSA Security Professionals (ISSM / ISSO), the DoD, Navy, National Nuclear Security Administration, Department of Energy National Labs, and to many other organizations

Please contact the ITDG with any questions regarding our training and consulting services.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program (ITP) Development, Management & Optimization Training Course Instructor
Insider Risk / Threat Vulnerability Assessment Specialist
ITP Gap Analysis / Evaluation & Optimization Expert
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG

Founder / Chairman Of The National Insider Threat Special Interest Group
Founder / Director Of Insider Threat Symposium & Expo
Insider Threat Researcher / Speaker
FBI InfraGard Member
LinkedIn NITSIG Group

Contact Information
561-809-6800
www.insiderthreatdefensegroup.com
jimhenderson@insiderthreatdefensegroup.com
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org