Center for Internet Security®

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Countering Ubiquitous Technical Surveillance

FACTS, FINDINGS, AND RECOMMENDATIONS FOR U.S. LAW ENFORCEMENT

November 2025

The National Working Group on Countering Ubiquitous Technical Surveillance

Contents

Message from the Working Group Chairs

In June 2025, the U.S. Department of Justice (DOJ) released a redacted audit regarding the Federal Bureau of Investigation's (FBI's) efforts to protect highly sensitive investigations and operations from technological compromise.[1] This threat, known as Ubiquitous Technical Surveillance (UTS), can enable threat actors with less technical sophistication to connect targeted entities to events or locations, potentially facilitating reconnaissance, harassment, or targeted acts of violence.

The audit highlights how one Mexican criminal enterprise used mobile device data and Mexico City's existing physical surveillance infrastructure to identify an FBI agent and the agent's key contacts — information the criminal enterprise used to threaten and, in some instances, kill potential confidential human sources (CHSs).

The surveillance of law enforcement personnel is not a new development, nor is it something that only happens abroad. Over the years, threat actors have collected and used information regarding law enforcement personnel and investigations to threaten officer safety and disrupt operations. However, in today's ecosystem, threat actors' ability to gather sensitive information is turbocharged by cyber intrusions and advanced technical capabilities.

UTS poses an existential threat to U.S. law enforcement. Its use by drug trafficking organizations, human smuggling rings, and organized criminal enterprises threatens both operational security and officer safety. Yet there is no authoritative guidance outlining how U.S. law enforcement can holistically prevent, identify, and mitigate UTS.

To fill that gap, the Center for Internet Security® (CIS®), in partnership with the Major County Sheriffs of America (MCSA) and the Association of Law Enforcement Intelligence Units (LEIU), initiated the National Working Group on Countering UTS. The working group, comprised of officials from law enforcement agencies across the United States, developed this product to serve as a comprehensive playbook for countering UTS.

Today's increasingly complex threat landscape is fueled by rapidly evolving commercial technologies, which fundamentally change how threat actors engage in malicious activities. In response, U.S. law enforcement must promptly update its policies and practices to protect critical investigations, ongoing operations, and law enforcement's greatest asset — its personnel — from the UTS threat.

John Cohen
Executive Director, Program for Countering Hybrid Threats
The Center for Internet Security

Megan Noland
Executive Director
Major County Sheriffs of America

Aaron Kustermann
Chair, Association of Law Enforcement Intelligence Units
Chief Intelligence Officer, Illinois State Police

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.

Executive Summary

The collection and analysis of data to link targeted individuals to events or locations, known as Ubiquitous Technical Surveillance (UTS), can undermine law enforcement operations and compromise officer, witness, and confidential human source (CHS) safety, leading the Central Intelligence Agency (CIA) to describe the UTS threat as "existential."[2] Center for Internet Security® (CIS®) analysts assess with high confidence[A] that foreign and domestic threat actors will likely exploit UTS data to undermine high-visibility law enforcement operations. This assessment is based on analysis of open-source reporting from the U.S. Department of Justice (DOJ), the U.S. Secret Service (USSS), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Department of Homeland Security (DHS), and various media outlets published between July 2019 and September 2025, in addition to insights gleaned from members of the National Working Group on Countering UTS.

While the threat posed by UTS is not new, recent technological advances "have made it easier than ever for less-sophisticated nations and criminal enterprises to identify and exploit vulnerabilities created by UTS," according to the DOJ.[3] This includes the emergence of open-source online tools, such as commodity malware and cyber exploitation resources, that enable threat actors to easily compromise UTS data. The threat is further compounded by U.S. law enforcement's reliance on various technologies that, if exploited, could reveal officers' locations, upcoming or ongoing enforcement operations, or sensitive information regarding pending cases and CHSs. These technologies include information technology (IT) systems, mobile devices, social media, online databases, radios, Bluetooth-connected devices, physical surveillance devices, and emerging technologies, including generative artificial intelligence (GenAI) and unmanned aircraft systems.

To mitigate the risks posed by UTS, U.S. law enforcement should consider incorporating cybersecurity controls focused on mission-critical technologies, stringent mobile device policies, online rules of behavior for all personnel and CHSs, and holistic counter-UTS programming.

Rigorous cybersecurity standards: Implement cybersecurity best practices, including the CIS Critical Security Controls® (CIS Controls®), for all law enforcement-related communications and IT systems to minimize risks of data compromise and exploitation.

Mobile device policies: Institute policies to protect mobile devices from malicious compromise, surveillance, and data collection, including strict location services settings and Wi-Fi and Bluetooth settings.

Online hygiene guidance: To foster online privacy awareness, provide all law enforcement personnel, CHSs, and their families with guidance regarding online behavior and social media privacy settings.

Counter-UTS programming: Conduct regular UTS vulnerability assessments, require recurring UTS training for all law enforcement personnel and CHSs, and create and practice a UTS incident response plan.

A The Center for Internet Security's estimative probability and analytic confidence standards can be found here.

Facts

UTS Definition and Overview

According to the FBI, UTS is "the widespread collection of data and application of analytic methodologies for the purpose of connecting people to things, events, or locations."[4] **Figure 1,** pictured below, summarizes the five categories of UTS data: travel, visual and physical, online, electronic signals, and financial.[5] Travel data includes unique identifiers related to flight records, hotel reservations, and international border crossings. Visual and physical data is information derived from cameras or physical surveillance infrastructure that can facilitate the identification of people, objects, or operations. Online data encompasses web browsing records and social media activity, while electronic signals involve the use of electronic devices, including cell phones and smart devices. Lastly, financial data includes transaction records and unique identifiers related to specified account holders.[6]

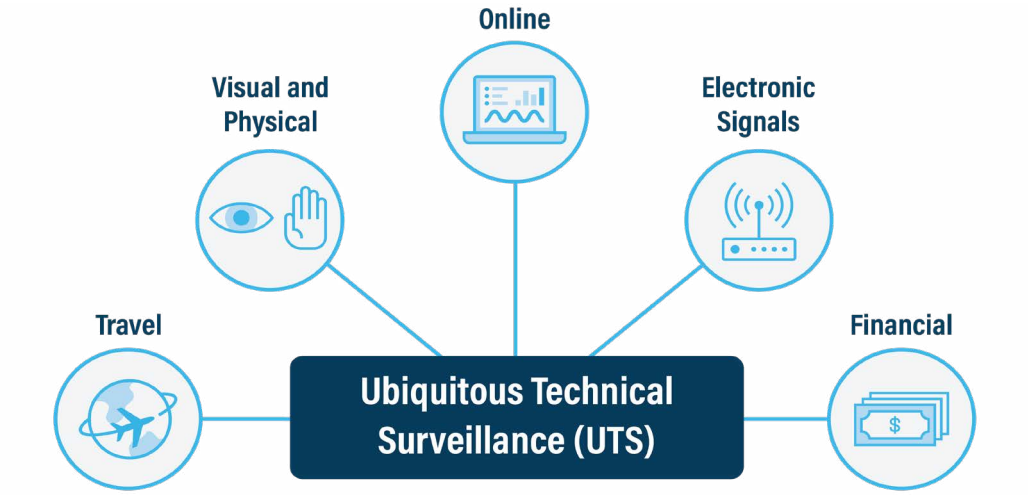

Figure 1. Ubiquitous Technical Surveillance Overview[56]

Findings

Hostile foreign adversaries, organized crime enterprises, and domestic threat actors can combine and aggregate UTS data from various sources to identify, track, or threaten law enforcement officers, witnesses, and CHSs; to detect, avoid, or undermine law enforcement operations; or to identify, adapt to, and evade common law enforcement investigative strategies. Potential vectors for UTS collection and exploitation include law enforcement IT systems, mobile devices, social media, online databases, radios, Bluetooth-connected devices, physical surveillance infrastructure, and emerging technologies such as GenAI and unmanned aircraft systems.

Law Enforcement IT Systems

State and non-state cyber threat actors continue to leverage a variety of malign cyber tactics to target U.S. law enforcement, including ransomware attacks and data breaches. Cyber attacks targeting law enforcement can disrupt mission-critical systems, such as public safety radios, computer-aided dispatch (CAD) systems, and public safety answering points (PSAPs), potentially resulting in significant operational and public safety impacts. Additionally, these cyber attacks provide an opportunity for threat actors to compromise and collect UTS data, including personally identifiable information (PII) related to law enforcement personnel, witnesses, or CHSs; investigative records; and internal administrative records.

- **Qilin ransomware attack compromised data from a Louisiana sheriff's office.** In September 2025, a Louisiana sheriff's office suffered a ransomware attack that disrupted inmate transfers, court appearances, and bail processing, forcing the office to resort to manual processes.[7] Qilin ransomware, a Ransomware as a Service (RaaS) operation first observed in 2022, later claimed responsibility for the attack.[8] Qilin claimed to have stolen 842 gigabytes of data from the sheriff's office, which reportedly included contract agreements, inmate intake records, expense information, and public police reports.[9,10]
- **LockBit ransomware attack compromised 77,000 police records, which included information related to witnesses.** In May 2024, the Russia-based ransomware group LockBit attacked the city of Wichita, Kansas, disrupting the city's network for more than two months.[11] The attack forced first responders, including police and firefighters, to initiate backup procedures while responding to emergency calls.[12] Following an investigation, city officials stated the ransomware attack "was focused on retrieving data from the Wichita Police Department," which included "potentially sensitive information about witnesses, victims, and suspects in 77,000 police cases."[13,14] The compromised data included names, addresses, dates of birth, email addresses, and credit card information.[15]
- **Data breach exposed "hundreds" of police officers' personal information.** In July 2019, a cyber threat actor compromised Los Angeles city computers, exposing the personal information of "about 20,000 applicants to the police department, including hundreds who are now sworn officers."[16] The data breach potentially compromised applicants' email addresses, dates of birth, last four digits of their Social Security Numbers, and passwords.[17]

Working Group Insights — Challenges Securing Law Enforcement IT Systems

Many small or medium-sized law enforcement agencies may not manage their own IT infrastructure and instead rely on municipal IT systems. According to a joint report by the Motorola Public Safety Threat Alliance (PTSA) and the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), "if not properly configured, segmented and secured, this network structure presents significant opportunities for [cyber threat actors] with access to enterprise IT environments to move laterally and access mission-critical systems." Working group members indicated this network structure can be problematic, since municipal IT personnel may not understand law enforcement's cybersecurity requirements or priorities.

Mobile Devices

In today's threat landscape, mobile devices can "become targeting beacons," leading U.S. Army Major General Curtis Taylor, the leader of the U.S. Army's National Training Center (NTC), to state, "this device [holding up a cell phone] is going to get our soldiers killed."[18] Mobile devices emit electronic signals and metadata, enabling threat actors to identify, track, threaten, or harm targeted entities. Organized crime enterprises and state-sponsored threat actors have exploited mobile device data to target senior U.S. law enforcement and government officials, to kill potential CHSs, and to gain critical insights into pending investigations.

- **Mexican cartel exploited cell phone data to identify law enforcement and threaten CHSs.** During the FBI's 2018 "El Chapo" investigation, an unnamed Mexican cartel hired a "hacker" to exploit electronic devices and identify "people of interest" in Mexico City, including an FBI Assistant Legal Attaché (ALAT). The threat actor used the ALAT's phone number to obtain geolocation and call data, and it gained access to Mexico City's camera system to surveil the ALAT and identify key contacts. The threat actor relayed the information to the cartel, who used the data to "intimidate, and in some instances, kill" potential CHSs, according to a DOJ audit.[19]
- **Chinese state-sponsored cyber threat group targeted U.S. telecommunications infrastructure to identify and track targeted entities.** In September 2025, the NSA, CISA, and the FBI, in addition to international partners, released a joint cybersecurity advisory (CSA) warning the Chinese state-sponsored group Salt Typhoon was targeting major telecommunications providers and internet service providers (ISPs), enabling Chinese intelligence services "to identify and track their targets' communications and movements around the world."[20] In late 2024, it was reported Salt Typhoon compromised nine U.S. telecommunications providers, targeting call records associated with senior U.S. government officials and "systems the federal government used for court-authorized network wiretapping requests."[21, 22, 23]
- **The USSS disrupted a "SIM farm" potentially capable of cellular surveillance.** In September 2025, the USSS announced it dismantled a SIM farm[B] network comprised of over 300 SIM servers and 100,000 SIM cards.[C, 24] The network was used to send anonymous telephonic threats to U.S. government officials, but it also could have been used to disable cell phone towers, conduct Denial of Service (DoS)[D] attacks, or facilitate encrypted communications between state-sponsored threat actors and criminal organizations, according to the USSS.[25] The SIM farm also could have allowed threat actors "to either intercept communications, eavesdrop on communications, or … clone devices," according to a former U.S. government official.[26]

Social Media

According to DHS, insecure social media practices "can increase exposure to risks ranging from cyber threats to reputational damage and sometimes physical harm."[27] Threat actors can leverage social media to conduct reconnaissance and gather critical information regarding targeted entities, including close contacts, location data, employment history, and PII. This information, if exploited, can compromise officer and CHS safety and undermine ongoing enforcement operations.

- **Fitness social networking application revealed the locations of high-profile officials and sensitive military information.** In October 2024, an investigation by the French news outlet Le Monde revealed how threat actors could use the Strava fitness application to track the locations of military personnel, security details, and high-profile officials. Le Monde

B SIM farms operate like a large collection of cell phones and can send mass calls and texts.
C Subscriber Identity Module (SIM) cards are small physical cards used to store cellular network and device identification information.
D During a Denial of Serve (DoS) attack, threat actors overwhelm a targeted network with traffic, intending to cause service disruptions.

analyzed the location data of security details, who tracked their workouts using public Strava accounts, to trace the movements of several world leaders, including a former and current U.S. president.[28] In January 2025, Le Monde also discovered 16 submarine crew members at a French naval base used public Strava accounts to track their workouts, inadvertently revealing sensitive patrol schedule information.[29]

- **Social media application TikTok sent U.S. user data to Chinese parent company.** In July 2024, the DOJ alleged TikTok employees sent sensitive U.S. user data to ByteDance, TikTok's China-based parent company, leading to U.S. user data being stored on China-based servers. The data reportedly included information regarding users' views on sensitive topics, including religion and gun control. The DOJ has "ongoing concern" China may be able to weaponize TikTok to impact U.S. national security, "a fear they say is made worse by demands that companies under Beijing's control turn over sensitive data to the government."[30] Due to China's policies, Chinese state-sponsored threat actors may be able to collect sensitive data regarding U.S. law enforcement officers, CHSs, and their families via the users' TikTok accounts.
- **Mexican cartels use social media to identify and target adversaries.** Cartels use social media as a tool to gather intelligence on rivals and plan armed attacks. For example, a "criminal operative" from Michoacán, Mexico, reportedly told the International Crisis Group his organization used Facebook to "identify enemy operatives, pull down personal information such as photographs and locations, and assemble lists of possible targets."[31] While this reconnaissance focused on rival criminal groups, cartels could use similar tactics to target law enforcement officers, CHSs, and their families.

Working Group Insights — Challenges Minimizing Officers' Social Media Presence

While many law enforcement personnel practice good social media hygiene, working group members outlined three scenarios that can unintentionally expose law enforcement personnel's sensitive information:

1. *Many younger law enforcement personnel have amassed a substantial online footprint before joining law enforcement organizations, making it more difficult to sanitize their online presence.*
2. *Law enforcement agencies often use social media for community engagement, and while community outreach is important, this activity can reveal law enforcement personnel's faces and full names. This exposure can be problematic if the personnel later work in an undercover capacity.*
3. *Oftentimes, law enforcement personnel's sensitive information is inadvertently exposed by family members' and friends' social media activity.*

Online Databases

Online databases are an essential tool for law enforcement investigations; however, online databases also serve as a critical repository of data that could be used for targeting. Ideologically motivated threat actors, domestic extortion groups, and organized crime enterprises have leveraged open-source, commercial, and law enforcement databases to conduct reconnaissance and identify potential targets. This information can facilitate online harassment, doxing,[E] and targeted acts of violence toward law enforcement personnel, CHSs, and their families.

- **Suspect allegedly used online databases to identify home addresses of targeted individuals prior to premeditated attacks.** In June 2025, a Minnesota man allegedly posed as a law enforcement officer and attacked two Minnesota lawmakers and their spouses, killing two and injuring two.[32] Prior to the attack, the man "took deliberate steps to research his victims" by "identifying several websites that allow users to search for the personal information of others, like home addresses and family member names," according to the criminal complaint.[33] While this attack allegedly targeted elected officials, threat actors could use similar techniques to research and identify law enforcement officers and their families.
- **Two men sentenced for breaching a law enforcement database, stealing PII, and threatening victims.** In May and June 2025, respectively, two men were sentenced for conspiracy to commit computer intrusion and aggravated identity theft. The men, who were members of a criminal group known as "ViLE," stole a law enforcement officer's login credentials to access a U.S. federal law enforcement database, which contained "nonpublic records of narcotics and currency seizures, as well as law enforcement intelligence reports," according to the DOJ. The men used information from the database to extort victims, threatening to post victims' PII on ViLE's public website unless victims paid to have their information deleted.[34]
- **Mexican cartels reportedly use intelligence software to track adversaries.** Mexican cartels reportedly gained access to Mexican intelligence and security software to track and target perceived enemies, according to a December 2023 report by VICE News. According to a source's statement to VICE News, the software allows users to "geolocate persons across the country in real time, access minute-to-minute location logs, and obtain official identification documents," and it reportedly "uses GPS technology to track a specific cell phone using either the phone number or the phone's ID." One source within the Cártel de Jalisco Nueva Generación told VICE News his organization had been using the software for at least six years, stating, "this is the easiest way to locate someone or to know about their relatives if they are hiding."[35]

Radios

U.S. law enforcement relies on radios for critical communications, emergency dispatch, and coordination and deconfliction, making radios an essential component of law enforcement operations. Law enforcement radios convey sensitive information regarding personnel's locations, ongoing operations, and victims and witnesses. If these communications are disrupted, intercepted, or broadcast via unencrypted channels, they can enable threat actors to impede investigations, expose operational tactics, or harm officers, victims, or witnesses.

- **DHS warns China-based technology firms are smuggling signal jammers into the United States.** In June 2025, DHS warned about increasing seizures of Chinese-manufactured signal jammers, which can interfere with critical law enforcement communications. Since 2021, U.S. Customs and Border Protection (CBP) has documented an 830% increase in seizures despite U.S. federal laws prohibiting signal jammers.[36] According to DHS, signal jammers "can be used to disrupt a range of radio frequency

E Doxing is when an individual's personally identifiable information (PII) is maliciously made public, typically online.

channels, and pose a threat to emergency response, law enforcement and critical infrastructure." For example, in December 2024 a threat actor employed a signal jammer to disrupt communications as law enforcement responded to a burglary.[37]

- **Threat actors listen to law enforcement's unencrypted radio communications, prompting encryption.** In March 2025, the Montgomery County Police Department (MCPD) in Maryland announced plans to fully encrypt all radio channels to ensure sensitive information is not broadcast to the public. Previously, unencrypted radio communications enabled the public to listen to MCPD communications via free police dispatch scanner applications and websites, inadvertently exposing victims and witnesses' PII to the public. The Assistant Chief of the department's Patrol Services Bureau also reported threat actors have previously intercepted the department's unencrypted radio channels, posing risks to officer safety, and potentially exposing information regarding operational tactics.[38]
- **Security researchers identify vulnerability in encrypted law enforcement and military radios.** In July 2023, security researchers from the firm Midnight Blue uncovered a vulnerability in encrypted radios that could allow threat actors to decrypt communications in under a minute, according to VICE News. The researchers conducted analysis of the TErrestrial Trunked Radio (TETRA) standard, a standard developed for mobile radios by the European Telecommunications Standards Institute (ETSI), which is used by global law enforcement, militaries, and critical infrastructure operators. The researchers uncovered a vulnerability in the encryption algorithm that would ultimately allow an attacker to passively decrypt communications in real time.[39] To mitigate this vulnerability, ETSI recommended users "deploy an end-to-end encryption solution on top of the flawed algorithm."[40] However, in August 2025, Midnight Blue identified "at least one implementation" of the recommended solution that still had similar vulnerabilities and could permit eavesdropping, according to WIRED.[41]

Working Group Insights — Portable Signal Jammers

Working group members expressed concern regarding portable signal jammers that plug into a vehicle's direct current (DC) 12-volt lighters. These devices can impede law enforcement's ability to track vehicles and communicate via radio during operations, including traffic stops, providing threat actors an avenue to evade detection and interdiction.

Per the Federal Communications Commission (FCC), federal law "prohibits the operation, marketing, or sale of any jamming equipment that interferes with authorized radio communications, including cellular and Personal Communication Services (PCS), police radar, and Global Positioning Systems (GPS)." In addition to disrupting law enforcement communications and operations, signal jammers can also pose severe risks to public safety by impeding emergency call capabilities.

Bluetooth-Connected Devices

Today, Bluetooth-connected devices are commonplace, from wireless headphones to smart home devices such as video doorbells, thermostats, and smart speakers. Bluetooth "enables two devices to connect directly without requiring supporting network infrastructure such as a wireless router or access point."[42] While these devices offer convenience and enhanced capabilities, Bluetooth-connected devices also serve as a potential vector for UTS exploitation. Bluetooth device vulnerabilities can enable threat actors to track law enforcement officers, CHSs, and witnesses, and they can facilitate the identification of ongoing law enforcement operations.

- **Body-worn camera (BWC) vulnerability could disclose law enforcement officers' locations.** In February 2025, U.S. Border Patrol (USBP) agents ceased using BWCs pending an investigation regarding an online claim BWCs could be detected via BLE Radar, a mobile application used to analyze surrounding Bluetooth Low Energy (BLE) devices. Social media posts claimed USBP agents could be detected "from at least 100 yards away."[43] Later that month, USBP resumed using BWCs after the "potential safety risk" concluded, according to a CBP statement provided to NewsNation.[44]

- **Design flaws in Bluetooth-enabled trackers could facilitate remote tracking.** Researchers discovered design flaws in Tile tags, tracking devices that use Bluetooth to broadcast their location, that could allow threat actors to track users, according to WIRED. When a user loses a Tile tag, they can use a mobile device application to query Tile servers for the item's last known location. The Tile system uses a network of devices to detect the broadcast of any nearby Tile tag, including the phones of other Tile users, Ring cameras, and Echo devices. Whenever a device detects a broadcast from a Tile tag, the tag's location, Media Access Control (MAC) address, and unique ID are sent to Tile's servers. Since this information is not encrypted, anyone with a Tile application or radio frequency antenna could intercept the information and track the tag or the user, according to the researchers. In a statement to WIRED, Tile's parent company Life360 said they had made "improvements" after learning of the design flaw but did not provide further information regarding the improvements.[45]
- **Smart home device vulnerabilities could expose law enforcement officers' home addresses.** In February 2024, Consumer Reports (CR) security researchers found doorbells manufactured by Eken Group, a Chinese smart home device manufacturer, exposed users' IP addresses and Wi-Fi network names to the internet without encryption. CR researchers found anyone with physical access to the doorbell could pair the device with an application on their smartphone, which could allow threat actors to remotely access the video feed and timestamped images of everyone who enters and exits the property.[46] Following the CR investigation, Eken Group released a firmware update to address the vulnerabilities.[47] Similar vulnerabilities within smart home devices could enable threat actors to surveil law enforcement officers and their families at their residences.

Physical Surveillance Devices

Security cameras can be found in many homes, businesses, intersections, and public transportation hubs, creating a comprehensive, and frequently vulnerable, physical surveillance infrastructure. These devices are designed for quick setup, "often skipping essential security configurations in the process, such as enabling user authentication or changing default credentials."[48] As a result, many physical security devices are left exposed to the internet, allowing threat actors to remotely view and capture video footage. Threat actors can exploit exposed video feeds or leverage strategically placed devices to surveil targeted entities, including law enforcement personnel and CHSs.

- **Security researchers identified over 40,000 security cameras with exposed video feeds.** In June 2025, BitSight security researchers scanned the internet for exposed security cameras and captured live footage from over 40,000 global cameras, including roughly 14,000 cameras in the United States. These cameras were likely exposed due to security misconfigurations, and they were found in offices, stores, factories, data centers, ATMs, public transportation corridors, and hospitals. BitSight observed threat actors selling access to exposed cameras on the dark web and stated, "attackers can use exposed cameras for espionage, stalking, extortion," and cyber attacks.[49]
- **Misconfigured automated license plate recognition (ALPR) system exposed records regarding passing vehicles.** In January 2025, a security researcher discovered over 150 misconfigured Motorola ALPR cameras, which are used to capture and record images of license plates, resulting in exposed video feeds and leaked records regarding passing vehicles. The ALPR devices "were likely exposed as they had not been set up on private networks, possibly by law enforcement bodies deploying them, and instead exposed to the internet without any authentication," according to the security researcher's statement to WIRED. Motorola told WIRED it was working with customers to address the exposed cameras.[50]
- **South American theft groups (SATG) use surveillance cameras to monitor targeted U.S. locations.** In May 2024, the Los Angeles County Sheriff's Department (LASD) published a situational awareness bulletin warning SATG operating in the United States

were concealing surveillance cameras in strategic locations, such as near residential homes, to monitor homeowners' patterns of life. These groups, often comprised of Chilean or Columbian nationals, "are highly organized criminal enterprises that travel from state-to-state committing burglaries and thefts," according to LASD.[51] While these cameras likely focused on identifying potential theft targets, SATG could also use the devices to track law enforcement response times and patrol patterns.

Emerging Technologies

Threat actors increasingly leverage GenAI and unmanned aircraft systems to facilitate malign activities, including UTS. GenAI has shifted how users access publicly available data and conduct research by providing answers to highly specific and targeted questions. Additionally, threat actors representing a broad range of ideological motivations, including cartels, human smugglers, and criminal organizations, have leveraged unmanned aircraft systems for surveillance. Unmanned aircraft systems pose unique challenges to law enforcement, since it can be difficult to identify whether these devices are being flown for benign or malicious purposes.[52]

- **AI tool used to identify masked U.S. Immigration and Customs Enforcement (ICE) agents.** An individual reportedly used an AI tool to reveal masked ICE agents' faces, which aided "public shaming" efforts online, according to Politico. The individual claimed his group can "reveal a face using AI, if they have 35 percent or more of the face visible," and reportedly identified at least 20 ICE agents that wore masks during recorded arrests. The individual claimed the tool uses screenshots from videos of ICE agents to generate images of what the agent could look like unmasked. The AI-generated images are then sent to volunteers who use reverse-image search engines to identify matching social media profiles. The technology was reportedly accurate in 40% of cases, and volunteers reportedly verify the results before publishing agents' names on the ICE List, a doxing site that provides the names, photos, occupations, or social media profiles of ICE personnel.[53]
- **Mexico-based cartels leverage unmanned aircraft systems to surveil U.S. law enforcement.** Mexico-based cartels are expected to continue incorporating surveillance tactics, including the use of unmanned aircraft systems, to monitor U.S. law enforcement along the southwest border, according to DHS's 2025 Homeland Threat Assessment.[54] In a July 2025 testimony for the Senate Judiciary Committee, a DHS official wrote, "CBP drone detections also led to the arrests of over 1,500 subjects along the southwest border, a clear indicator that [cartels] are adopting the use of drones into their tactics as a means of surveilling and evading CBP agents and officers and other law enforcement."[55]

Recommendations

To mitigate the risks posed by UTS, U.S. law enforcement should consider incorporating cybersecurity controls focused on mission-critical technologies, stringent mobile device policies, online rules of behavior for all personnel and CHSs, and holistic counter-UTS programming.

Rigorous Cybersecurity Standards

1. **Adopt the CIS Controls for all information technology systems.**
   - Prioritize CIS Controls Implementation Group 1, which represents a minimum information security standard for all organizations.
   - For mission-critical systems, implement CIS Controls Implementation Group 2 and Implementation Group 3, which provide additional CIS Safeguards to help security practitioners cope with increased operational complexities.
   - Law enforcement agencies that use municipal resources for IT and cybersecurity support should maintain operational alignment with their municipal Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and IT and information security teams to ensure their agency possesses the foundational level of cybersecurity required to mitigate today's threats. See CIS's blog, 5 Cyber Questions Sheriffs & Police Chiefs Should Ask, for additional guidance.
2. **Implement robust data protection measures (CIS Control 3).**
   - Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.
   - Encrypt data on all end-user devices containing sensitive or confidential information.
3. **Harden systems that collect or process UTS data (CIS Control 4).**
   - Establish and maintain the secure configuration of enterprise assets that collect, process, or maintain UTS data (including end-user devices, network devices, Internet of Things (IoT) devices, and servers).
   - For additional guidance securing IoT devices, see CIS's Internet of Things Companion Guide.
4. **Manage access to all devices and networks (CIS Control 6).**
   - Require multi-factor authentication (MFA) on all devices and third-party applications. Also, require MFA for remote network access and administrative access.
   - Establish an access granting/revoking process to ensure users only have access to the data or enterprise assets appropriate for their role.
   - Collect and audit access logs to ensure critical systems and information are only being accessed for appropriate and approved needs.

Mobile Device and Radio Policies

5. **Keep official and personal communications separate.**
   - If possible, provide law enforcement personnel and CHSs with separate mobile devices for all mission-related emails, text messages, and data storage to minimize data spillage onto personal devices.

- Issue Faraday bags for all devices communicating with CHSs or witnesses. Also, keep devices in the Faraday bags when not in operational use.
- Review the CIS Controls Mobile Companion Guide to secure phones, tablets, and mobile applications.

6. **Require law enforcement personnel to adopt specific mobile device settings and practices.**
   - If possible, require law enforcement personnel to disable Wi-Fi and Bluetooth on all devices while on duty or within law enforcement facilities to minimize electronic metadata.
   - Law enforcement agencies should use a virtual private network (VPN) for all mobile devices.
   - Instruct law enforcement personnel and CHSs to disable location services for applications on their mobile device to limit location data collection. This includes disabling the Identifier for Advertisers (IDFA) on iOS devices and the Android Advertising ID (AAID) on Android devices, unique alphanumeric numbers that allow advertisers to track user activity.
   - Instruct law enforcement personnel to check mobile device settings in conjunction with any software updates to ensure data collection settings or agreements have not changed.
   - Charge mobile devices using charge-only cables and do not charge devices via public USB ports.
7. **Audit mobile applications prior to download and installation (CIS Control 2).**
   - Before installing any application, review its privacy policies to understand the types of data each application collects. Additionally, conduct a risk assessment prior to integrating any applications, particularly non-U.S. based applications, into organizational processes.
   - Implement an Acceptable Use Policy (AUP) outlining which applications are authorized for business devices.
   - Consider the risks associated with uploading data to third-party applications, including GenAI applications.
8. **Encrypt all radio communications.**
   - Law enforcement organizations should encrypt all radio channels, including dispatch channels, and should use the most up-to-date encryption standards and algorithms.
   - If an encrypted radio is lost or stolen, law enforcement organizations should immediately re-key all radios to update the encryption keys and prevent the misplaced radio from accessing restricted communications.

Online Hygiene Guidance

9. **Provide guidance regarding social media best practices.**
   - Instruct law enforcement personnel, CHSs, and their families to maintain private settings on personal social media accounts and remove locations from all online posts and photos. For additional guidance, see CIS's Guide to Managing Your Online Presence.
   - Create social media profiles using new, separate email addresses, which can minimize connections between users' existing information and social media activity.
   - Disable social media applications' contact sharing features to avoid publicizing personal contacts.
   - Use strong passwords for all social media accounts, regularly change passwords, and, where possible, enable MFA.

10. **Remove PII from online data sources.**
    - Encourage law enforcement personnel, CHSs, and their families to sanitize their online presence by deleting inactive social media accounts, conducting open-source searches of their name and other personal information, opting out of data broker websites, and requesting removal of personal information from real estate websites.
    - If personnel use commercial services to remove their PII from online sources, ensure the commercial service is based in the United States to avoid exposing PII on overseas servers.
11. **Organize family online safety programs.**
    - Organize training programs to educate law enforcement personnel's families on digital hygiene and online safety best practices.
    - To help educate children regarding online safety, parents can review CIS's From Both Sides - A Parental Guide to Protecting Your Child's Online Activity.

Counter-UTS Programming

12. **Conduct continuous UTS vulnerability assessments (CIS Control 7).**
    - Evaluate all information and communication systems, along with key technologies, for potential UTS vulnerabilities.
    - Document all UTS vulnerabilities in a formalized internal report, prioritize the vulnerabilities based on exploitation likelihood and potential impact, and identify mitigation strategies for prioritized vulnerabilities.
    - Review and adjust the UTS vulnerability assessment on a regular basis to audit any new technologies; address any newly identified threat actor tactics, techniques, and procedures (TTPs); and document new mitigation strategies.
13. **Develop guidelines for foreign travel and foreign delegation visits.**
    - Develop guidance for international travel to ensure the safety and security of personnel, CHSs, and electronic devices. This guidance should include pre- and post-travel security briefings as well as guidelines for inspecting, wiping, and reloading all department-issued electronic devices that leave the United States.
    - Create a protocol for events and delegation visits involving foreign dignitaries, diplomats, and government officials to mitigate counterintelligence risks. This protocol should include coordination with federal law enforcement partners and local fusion centers as well as physical security controls and electronic device policies.
14. **Require recurrent UTS training (CIS Control 14).**
    - Mandate regular and updated UTS training for all law enforcement personnel regarding technical compromise, secure communications, and safe CHS handling.
    - Educate CHSs on the risks posed by UTS and provide mitigation measures that align with your organization's UTS vulnerability assessment and incident response plan.
15. **Create a UTS incident response plan (CIS Control 17).**
    - Develop a UTS incident response plan addressing potential vectors of compromise and the malicious use of UTS data in addition to delineating clear lines of responsibility, communication, and deconfliction in the event of a UTS incident.

CIS Resources and Services

CIS offers a range of free resources and paid services to help U.S. law enforcement organizations secure mission-critical technologies, understand today's complex threat environment, and foster online safety and privacy awareness. For additional information regarding CIS's services, contact CIS here.

Free Resources

- CIS Critical Security Controls® (CIS Controls®): A prescriptive, prioritized, and simplified set of cybersecurity best practices designed to help organizations improve their cybersecurity posture.
- CIS Controls Mobile Companion Guide: Guidance for applying the CIS Controls to Google Android and Apple iOS environments.
- CIS Benchmarks®: Community-developed secure configuration recommendations for hardening 100+ technologies across more than 25 vendor product families against evolving cyber threats.
- CIS's Guide to Managing Your Online Presence: Provides actionable guidance to protect your personal information and secure your online privacy.
- CIS's From Both Sides - A Parental Guide to Protecting Your Child's Online Activity: A comprehensive guide crafted to teach children safe online practices and help parents to understand the hazards of harmful online behaviors.

Paid Services

- CIS Hardened Images®: Provide virtual images pre-hardened to the CIS Benchmarks, creating a secure, on-demand, and scalable computing environment.
- ThreatWA™: Warning and analysis intelligence service, which includes weekly intelligence report covering cyber threats by state and non-state threat actors, physical threats facilitated by online activity, and online activity by foreign threat actors to incite, inform, or facilitate illegal activity.
- CIS SecureSuite® Membership: Comprehensive set of cybersecurity resources and tools to streamline your implementation of the CIS Controls and CIS Benchmarks.
- Multi-State Information Sharing and Analysis Center® (MS-ISAC®) Membership: Provides members with incident response support, cyber threat intelligence, and real-time information sharing programs.
- Secure Cyber City™: Provides U.S. cities and communities with customized cybersecurity measures, dynamic cyber threat intelligence sharing, and community awareness campaigns to holistically enhance participants' defenses against today's evolving threats.
- Vulnerability Assessments: Provides organizations with a cost-effective solution for network auditing and vulnerability management. Services include network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking according to business risk.
- Penetration Testing: Simulates a real-world cyber attack, allowing organizations to safely review the security posture of their web applications and networking devices.

References

1 https://oig.justice.gov/sites/default/files/reports/25-065_t.pdf

2 https://oig.justice.gov/sites/default/files/reports/25-065_t.pdf

3 https://oig.justice.gov/sites/default/files/reports/25-065_t.pdf

4 https://oig.justice.gov/sites/default/files/reports/25-065_t.pdf

5 https://oig.justice.gov/sites/default/files/reports/25-065_t.pdf

6 https://oig.justice.gov/sites/default/files/reports/25-065_t.pdf

7 https://www.wwltv.com/article/news/local/orleans/orleans-parish-sheriffs-office-hit-by-ransomware-attack/289-a39e1128-4e99-4161-b8cc-0d753d7431bd

8 https://www.axios.com/2025/09/15/new-orleans-sheriff-ransomware-attack-data-leak

9 https://www.axios.com/2025/09/15/new-orleans-sheriff-ransomware-attack-data-leak

10 https://www.cbsnews.com/news/cybercriminals-demanding-ransom-to-free-up-parts-of-new-orleans-area-sheriffs-office-computer-systems/

11 https://www.kmuw.org/news/2024-09-19/city-increasing-security-after-thousands-of-wichita-police-records-are-compromised-in-cyber-attack

12 https://www.kansas.com/news/politics-government/article288397380.html

13 https://www.kake.com/home/city-ransomware-attack-targeted-wichita-police-department-exposing-77-000-case-files/article_55cd1fd4-7604-11ef-945b-c712cff71ca1.html

14 https://www.govtech.com/security/wichita-kan-cyber-incident-limited-to-police-records

15 https://www.kake.com/home/city-ransomware-attack-targeted-wichita-police-department-exposing-77-000-case-files/article_55cd1fd4-7604-11ef-945b-c712cff71ca1.html

16 https://www.latimes.com/california/story/2019-07-29/lapd-applicants-data-breach

17 https://www.latimes.com/california/story/2019-07-29/lapd-applicants-data-breach

18 https://medium.com/@david_n_cook/when-cell-phones-kill-digital-discipline-and-the-future-of-sof-obscurity-e0252e136e77

19 https://oig.justice.gov/sites/default/files/reports/25-065_t.pdf

20 https://media.defense.gov/2025/Aug/22/2003786665/-1/-1/0/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.PDF

21 https://techcrunch.com/2024/10/07/the-30-year-old-internet-backdoor-law-that-came-back-to-bite/

22 https://techcrunch.com/2025/08/27/fbi-says-chinas-salt-typhoon-hacked-at-least-200-us-companies/

23 https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b

24 https://www.secretservice.gov/newsroom/releases/2025/09/us-secret-service-dismantles-imminent-telecommunications-threat-new-york

25 https://www.secretservice.gov/newsroom/releases/2025/09/us-secret-service-dismantles-imminent-telecommunications-threat-new-york

26 https://apnews.com/article/unga-sim-farm-threat-explainer-5274ccc927ab180a1d5e0ffd475ed7c9

27 https://www.dhs.gov/sites/default/files/2025-04/25_0306_fps_social-media-privacy-settings-safety.pdf

28 https://apnews.com/article/biden-trump-macron-bodyguards-security-strava-0a48afca09c7aa74d703e72833dcaf72

29 https://www.lemonde.fr/en/videos/article/2025/01/13/stravaleaks-dates-of-french-nuclear-submarine-patrols-revealed-by-careless-crew-members_6737005_108.html

30 https://www.cbsnews.com/news/tiktok-lawsuit-justice-department-collected-views-bytedance/

31 https://www.crisisgroup.org/latin-america-caribbean/mexico/b50-fear-lies-lucre-how-criminal-groups-weaponise-social-media-mexico

32 https://www.justice.gov/opa/pr/after-two-day-manhunt-suspect-charged-shooting-two-minnesota-lawmakers-and-their-spouses

33 https://www.documentcloud.org/documents/25977053-criminal-complaint-us-vs-vance-luther-boelter/

34 https://www.justice.gov/usao-edny/pr/two-men-sentenced-prison-aggravated-identity-theft-and-computer-hacking-crimes

35 https://www.vice.com/en/article/mexican-cartels-government-security-software-track-target-enemies/

36 https://www.fcc.gov/general/jammer-enforcement

37 https://www.dhs.gov/news/2025/06/18/homeland-security-warns-about-spike-china-based-technology-firms-smuggling-signal

38 https://bethesdamagazine.com/2025/03/28/montgomery-county-police-encrypt-radio-transmissions/

39 https://www.vice.com/en/article/backdoor-in-police-radios-tetra-burst/

40 https://www.wired.com/story/encryption-made-for-police-and-military-radios-may-be-easily-cracked-researchers-find/

41 https://www.wired.com/story/encryption-made-for-police-and-military-radios-may-be-easily-cracked-researchers-find/

42 https://www.intel.com/content/www/us/en/products/docs/wireless/what-is-bluetooth.html

43 https://www.newsnationnow.com/us-news/immigration/border-coverage/border-patrol-agents-body-cameras/

44 https://www.newsnationnow.com/us-news/immigration/border-coverage/border-patrol-agents-resume-body-cameras/

45 https://www.wired.com/story/tile-tracking-tags-can-be-exploited-by-tech-savvy-stalkers-researchers-say/

46 https://www.consumerreports.org/home-garden/home-security-cameras/video-doorbells-sold-by-major-retailers-have-security-flaws-a2579288796/

47 https://www.consumerreports.org/media-room/press-releases/2024/04/eken-fixes-security-issues-in-video-doorbell-cameras-after-consumer-reports-investigation/

48 https://enablement.bitsight.com/sh/570339668395124546/assets/?id=570339016365373055

49 https://enablement.bitsight.com/sh/570339668395124546/assets/?id=570339016365373055

50 https://www.wired.com/story/license-plate-reader-live-video-data-exposed/

51 https://x.com/LHSLASD/status/1795555305981411824

52 https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf

53 https://www.politico.com/news/2025/08/29/ai-unmasking-ice-officers-00519478

54 https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf

55 https://www.judiciary.senate.gov/imo/media/doc/94f53245-d172-92ba-152b-06bc9ee00a50/2025-07-22%20-%20Testimony%20-%20Willoughby%20-%20final.pdf

56 https://oig.justice.gov/sites/default/files/reports/25-065_t.pdf