National Security Encryption

Adoption of Keystroke-Level Encryption Across FBI Communications and Operational Systems

Dr. Diane M. Janosek

Dr. Janosek's analysis below independently validates the need for keystroke encryption in all national security and law enforcement digital communication devices to protect data at creation.

The United States of America remains committed to national security, economic stability, and the protection of its citizens. The Executive Branch, including the Department of Justice and the Federal Bureau of Investigation, must ensure that law enforcement and national security personnel enjoy the highest assurance of confidentiality, integrity, and availability of sensitive information.

The contemporary threat environment, with sophisticated nation-state adversaries, cybercriminal enterprises, illicit communications networks, and domestic violent extremism, requires federal agencies to adopt the most rigorous and forward-looking security protections. Traditional encryption of data at rest and in transit, while foundational, does not sufficiently address risk to data at the point of creation. Sensitive intelligence, operational directives, and investigative communications remain exposed when entered via keyboards or mobile text interfaces prior to encryption.

Encryption that begins only after data is created is no longer sufficient. In law enforcement and national security operations, the keyboard is the first battlefield. Protecting information at the point of creation through keystroke-level encryption must be the first line of defense to safeguard missions, personnel, and the public.

Strategic and Policy Context

Longstanding executive policies have directed agency heads to manage cybersecurity risk across the federal enterprise and modernize legacy information technology systems to defend against unauthorized access and data compromise.[1] Cyber criminals, bad actors, and foreign adversaries seek to exploit vulnerabilities in information and communications technology platforms to bring about "catastrophic effects" on national security and economic interests. Thus, the assessment of hardware, software, and services for systemic risks was mandated.[2] In 2025, The White House directed federal efforts to advance secure software development, post-quantum cryptography standards, and other modernized protections while revising legacy cyber policy frameworks.[3]

[1] The Trump Administration's Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 11, 2017) underscored President Trump's commitment that all federal IT and data "should be secured responsibly using all United States Government capabilities," and he expected all agencies to be accountable for risk management commensurate with potential harm.

[2] The Trump Administration's Executive Order on Securing the Information and Communications Technology and Services Supply Chain (May 15, 2019).

[3] The Trump Administration's Executive Order Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Prior Orders (June 6, 2025). This order directs multiple agencies, including DHS, NSA, NIST, and DoD, to update security practices that counter emergent threats posed by state and non-state actors.

Why Traditional Encryption and MFA Are No Longer Sufficient on Their Own

Multi-factor authentication (MFA) is widely deployed across government systems and is an essential security control. However, MFA assumes the integrity of the endpoint device on which credentials and authentication codes are entered. When a keylogger is present, usernames and passwords can be captured as they are typed. If an attacker has also compromised a secondary authentication channel, such as email, the same interception techniques can capture one-time passcodes or verification links. In such cases, attackers can defeat MFA without breaching encrypted networks or databases, often remaining undetected for extended periods.

For national security systems, this creates a particularly dangerous condition: adversaries gain legitimate credentials, operate as authorized users, and quietly access sensitive communications, intelligence products, and operational information. This type of access is far more difficult to detect and remediate than traditional network intrusions.

Why End-to-End Encryption Must Begin at the Keystroke

National security depends on the confidentiality, integrity, and availability of sensitive information across its entire lifecycle. While government agencies and national security institutions have invested heavily in encrypting data at rest and in transit, recent and historical cyber incidents demonstrate that a critical vulnerability remains insufficiently addressed: the moment data is created.

The Unprotected Point of Creation: A Persistent National Security Vulnerability

The vulnerability of sensitive information at the point of entry has been repeatedly exploited in high-profile national security incidents. Salt Typhoon, a Chinese state-aligned hacking group implicated in both global telecom breaches and the recent congressional staff email compromise, is known to deploy custom malware payloads including credential dumpers and keylogging components to steal passwords and maintain persistent access once inside targeted networks.[4] The Financial Times and Reuters report this month that this same group has recently breached email systems of House committee staffers, underscoring how these credential-capture techniques continue to threaten sensitive U.S. systems.[5] Foreign adversaries no longer need to defeat hardened networks or break encryption algorithms to obtain sensitive information. They simply wait for data to be typed.[6]

Why Endpoint Detection and Response (EDR) & VPNs Are Also Insufficient on Their Own

Endpoint Detection and Response (EDR) tools and Virtual Private Networks (VPNs) play important roles in modern cybersecurity architectures, but they do not address the fundamental

[4] Salt Typhoon Exposed: A Deep Dive Into a State-Sponsored Cyber Threat - PlexTrac (Feb. 27, 2025).

[5] China hacked email systems of US congressional committee staffers, FT reports | Reuters (Jan. 7, 2026).

[6] By encrypting data the moment of entry, national security institutions can eliminate a long-standing vulnerability that has enabled some of the most consequential cyber intrusions in recent history. This protection is especially important in environments involving shared systems, remote access, mobile devices, and complex interagency collaboration.

vulnerability at the point of data entry. EDR solutions are designed to detect suspicious behavior, anomalies, or known malicious activity on an endpoint over time. While effective for identifying threats after they manifest, EDR is inherently reactive. By the time anomalous behavior is detected or an alert is generated, a keylogger may have already captured credentials, authentication tokens, or sensitive communications at the keyboard, data loss that cannot be reversed.

Similarly, VPNs provide strong protection by encrypting data in transit between a user and a network. However, VPNs do not protect the integrity of credentials themselves. If a password or authentication code is captured by a keylogger before the VPN tunnel is established, or while a user is legitimately connected, encryption in transit offers no protection. Once valid credentials are stolen, adversaries can authenticate through the VPN as authorized users, rendering the encrypted tunnel ineffective as a defensive control.

In both cases, EDR and VPNs operate *after* the moment of creation or authentication. Neither prevents data from being intercepted at the keyboard.

Operational Imperative

A critical gap remains if action is not taken: insufficient protection of data at the point of entry. Keystroke-level encryption ensures that information is secure at the moment of creation, before keyboard buffer, system memory, or transmission layers can be intercepted or logged by adversarial software. This capability is especially salient given the operational realities of law enforcement field communications, mobile device usage, and rapid analytic exchange across secure and unclassified networks.

The adoption of patented, U.S.-based keystroke encryption fulfills a strategic necessity. In an environment where encrypted communication is standard for transit and storage, protecting data at the genesis point aligns directly with executive policies mandating risk management across the IT lifecycle. This approach adheres to federal guidance to modernize cybersecurity postures and to mitigate vulnerabilities that foreign and domestic adversaries exploit, particularly as geopolitical competitors seek to degrade U.S. security capabilities through cyber operations.

National security and economic security are inherently linked.[7] Exploitation of vulnerabilities in federal law enforcement communications systems has direct implications for economic espionage, intellectual property theft, and critical infrastructure compromise. The FBI, the lead agency for federal law enforcement, domestic counter-intelligence and the investigation of cyber threats, should adopt available encryption practices that address the evolving nature of risk and align with executive guidance on enterprise-wide risk management and secured IT modernization.

[7] America's allies and trading partners likewise need secure communications and devices to prevent economic espionage and illicit activity. Trading partners cannot introduce products and services with vulnerabilities into the United States' economy. A secure supply chain and secure communication pathways between countries' law enforcement agencies is imperative. National security and economic security are inherently linked, especially in supply chains with trading partners.

Recommendation

Adversaries do not wait for data to be encrypted in transit or at rest: they exploit it at the moment it is entered. Keystroke-level encryption closes a critical security gap and reflects the kind of forward-leaning, risk-based protection that modern law enforcement and national security demand.

The Federal Bureau of Investigation should, when at all possible, implement keystroke-level encryption across all applicable communication devices and platforms used by personnel engaged in investigative, counter-terrorism, and national security operations. This adoption should be directed through formal policy guidance and integrated into the FBI's enterprise security architecture contemporaneously with other federally directed cybersecurity modernization efforts.

Today is not the time to permit avoidable exposure of sensitive information. Those who protect the nation and its freedoms deserve the most advanced protections available. Keystroke-level encryption is a pragmatic and strategically aligned step toward fulfilling that obligation.

Our agents operate on the front lines of national security and federal law enforcement, often under constant threat from sophisticated adversaries. Failing to secure communications at the point of creation exposes both missions and lives. Providing keystroke-level encryption is not optional; it is a responsibility we owe to those who risk everything in service to this nation.
Dr. Janosek, January 2026

Dr. Diane M. Janosek[8]

[8] Dr. Diane M. Janosek, Esq., PhD, has over 25 years of leadership in national security and cybersecurity, including senior roles at the National Security Agency (NSA) and direct reporting to The White House and the Pentagon. She is an international cybersecurity expert and author. Janosllc.com