



THREAT BRIEF

FEDERAL EXECUTIVE PROTECTION

The Executive Is the Perimeter

The attack surface for federal executives has moved to their identity, contact graph, and exposed personal data. A domain- and perimeter-centric program sees fewer than one in twenty of the impersonations aimed at a federal principal. Covers January 2024 to September 2026.

SCOPE

US federal executives and protective communities

REPORTING WINDOW

01JAN2024 to 30SEP2026

ISSUED

30SEP2026

PREPARED BY

DJ Peterson
Doppel SECR

01 THE FINDING

DOMAIN-FIRST VIEW

< 1 in 20

A protective posture built around the network perimeter and lookalike domains sees fewer than one in twenty of the impersonations aimed at a federal executive.

Across Doppel customers that monitor social media, paid ads, and domains, executive impersonation concentrates on the surfaces that posture watches least. Most coordinated campaigns Doppel tracks never touch a domain at all.

EXECUTIVE IMPERSONATION ON SOCIAL MEDIA

89% average per customer

EXECUTIVE IMPERSONATION ON PAID ADS

6% average per customer

EXECUTIVE IMPERSONATION ON DOMAINS

2% average per customer

CAMPAIGNS THAT NEVER TOUCH A DOMAIN

64% of coordinated campaigns Doppel tracks

The defining shift of this window is the move from consumer-grade brand impersonation to the targeting of named officials and the institutions they represent. Actors clone a federal executive's voice, fabricate video, and impersonate agencies to reach the executive's peers, staff, and the public, then move them onto encrypted messaging. Impersonation is no longer only a fraud and reputation problem. It is now a reconnaissance and access problem that feeds physical-security risk. The public numbers track the shift. According to the [FBI IC3](#), government-impersonation fraud losses nearly doubled to \$797.9M in 2025, and the [US Capitol Police](#) recorded a record 14,938 threats to Members of Congress. The pace has held into 2026. The [FBI reported](#) in September nearly 61,000 complaints of law-enforcement and government impersonation between January 2025 and July 2026, with losses above \$1.6B, and warned that AI now lets scammers appear as deepfake officials on video calls.

The enabler underneath it did not change. Personal data is cheap to acquire and slow to remove, and the 2020 attack that killed a federal judge's son remains the template for how online exposure becomes physical harm. The posture in one phrase: identity-led, AI-accelerated, and online-to-offline.

THE NUMBERS THAT FRAME THE WINDOW

GOVERNMENT-IMPERSONATION LOSSES, 2024 TO 2025

+97% nearly doubling to \$797.9M

THREATS TO MEMBERS OF CONGRESS IN 2025

14,938 an all-time record, up 58%

02 ONE CAMPAIGN, MANY SURFACES



Consider how impersonation of a single senior military leader actually appears in the wild. The officer's official portrait and biography, public by virtue of the role, are cloned into dozens of fake profiles across Facebook, Instagram, and WhatsApp. The same identity anchors romance and investment lures that move targets onto Telegram, and the operators register lookalike domains and run paid ads to widen the funnel. The likeness of a single retired four-star officer has been cloned into [hundreds of fake accounts](#) that persist for years.

A tool watching domains sees two or three lookalike registrations and closes them. It never sees the other assets, on the surfaces where the impersonation actually lives, that belong to the same operator. Correlating them into one campaign through shared infrastructure, personas, and content is what lets the operation be dismantled as a whole rather than one artifact at a time.

WHAT A DOMAIN-ONLY VIEW SEES

A handful of lookalike domains, taken down one at a time. The social, messaging, and ad assets that carry most of the campaign stay live, and the operator re-registers.

WHAT THE CAMPAIGN ACTUALLY IS

One operator, one identity, many surfaces, linked into a single campaign. Across Doppel's threat-graph campaigns, 64% never touch a domain at all.

03 WHERE THE THREAT ACTUALLY LIVES



Impersonation of an individual does not live on domains. For the average customer, close to nine in ten executive impersonations appear on social media and about two percent on domains, the inverse of a domain-first monitoring posture. Brand impersonation is more evenly split, with roughly a third on domains, which makes the executive case distinct. An executive's exposure concentrates on exactly the surfaces a perimeter-centric program watches least.

Why a commercial dataset reads across to federal principals. These shares come from Doppel's commercial customer base, not federal systems. The read-across is direct. The adversaries, surfaces, and tradecraft are the same ones documented against federal executives in the public record. A senior official's exposure differs from a corporate brand's in degree (the personal-data and physical-safety stakes are higher), not in kind.

04 THE THREAT, ACROSS FEDERAL EXECUTIVES

AI VOICE IMPERSONATION OF OFFICIALS

The [FBI](#) warned twice in 2025 that actors clone senior officials' voices and spoof their display names to reach the officials' peers and staff, then move them onto Signal, Telegram, or WhatsApp. As [NPR reported](#), a June to July 2025 case impersonated the Secretary of State to foreign ministers, a governor, and a Member of Congress.

DOXXING AND DATA-BROKER EXPOSURE

People-search brokers convert a public name, or even a face, into a home address in minutes. In 2025 this fed a [purpose-built site](#) publishing immigration-enforcement personnel and, as [The Record reported](#), a state-lawmaker assassination whose attacker listed eleven data-broker services in his notebook. Exposure is the root enabler of nearly every downstream tactic.

SWATTING AND ONLINE-TO-OFFLINE ESCALATION

Falsified emergency calls send armed police to an executive's home. A commoditized swatting-for-hire market runs on encrypted channels. The [DOJ prosecuted](#) one ring that targeted more than seventy-five officials, and a [Supreme Court justice's home was swatted](#) in May 2026.

FABRICATED VIDEO AND SYNTHETIC MEDIA

Manipulated video of named federal figures is now recurrent, spanning foreign influence operations, election-related fabrications, and crypto-scam lures. Documented 2024 to 2026 cases include a [State Department spokesperson](#), presidential and cabinet figures, and Members of Congress. Video lags voice in impact today, but the case count is rising.

The pattern expresses differently by community. The **judiciary** shows the clearest full chain, from broker-sourced addresses to doxxing, swatting, and, in the landmark 2020 case, a fatal home attack. The [US Marshals Service](#) logged 564 threats against federal judges in FY2025 and [448 more in FY2026](#) as of 15SEP2026, and [Supreme Court Police project](#) a further increase in 2026. **Immigration-enforcement personnel** saw the sharpest 2025 surge in doxxing and online-to-offline threats. **Senior military leaders** are impersonated at scale for fraud, and the reflexive twist is that agencies which [warn about impersonation](#), including Army CID, are themselves impersonated. **Members of Congress** absorb the highest raw volume of threats. **Executive-branch protectees** face the physical end directly, including two 2024 assassination attempts and a [2026 checkpoint shooting](#) near senior officials.

05 WHAT A MODERN POSTURE REQUIRES

IMMEDIATE (0-30 DAYS)

1

Treat the contact graph as the protected surface. The campaign also targets the people around the principal, including staff, family, and peers. Give that circle a verification protocol for any unexpected request that appears to come from the principal, a code word plus a known-channel callback. This is the highest-leverage control against the AI-voice technique the FBI has warned about twice.

2

Collapse exposure at the source. Run continuous data-broker and people-search removal for principals and high-exposure staff, and measure it by listings removed and kept down, not one-time opt-outs. Broker republication is automated, so removal that does not repeat is theater.

THIS QUARTER (30-90 DAYS)

3

Instrument the surfaces where impersonation lives, and fuse the tickets. Measure external-threat coverage by surface, and stand up a single correlated view across cyber, fraud, protective intelligence, and physical security so a coordinated campaign is seen as one operation and online precursors inform physical posture.

THIS HALF (90-180 DAYS)

4

Pre-position enforcement, and use the legal levers. Establish takedown and abuse-reporting relationships and an evidence-package workflow before an incident, so a doxxing site or impersonation cluster can be interdicted in hours. Where covered, use judicial- and official-privacy statutes to compel broker removals. In August 2026, [New Jersey's Supreme Court held](#) that a broker is liable under Daniel's Law once a removal notice lapses, without proof of fault. Share indicators across peer agencies.

THE STANDARD TO HOLD

Detection alone does not reduce exposure. What matters is how quickly a campaign is dismantled across every surface it touches, and whether those surfaces are tied to one operation instead of worked as isolated tickets. Any program protecting federal executives should be able to report time to takedown on each surface and the share of findings linked to a known campaign. For reference, Doppel publishes its own [enforcement benchmarks](#).

06 OUTLOOK AND CAVEATS

Outlook. We assess that threat activity against federal executives will remain identity-led, AI-accelerated, and online-to-offline, at a sustained elevated level through the next two quarters. Impersonation, doxxing, and swatting are cheap, effective, and low-risk for the actor, which favors persistence. We expect AI impersonation to keep rising, doxxing and swatting to stay elevated, and physical incidents to remain episodic and severe. The direction is clear. The magnitude is the open question.

Caveats. Attribution for impersonation activity is frequently unresolved, so we separate observation from assessment throughout. The US Secret Service and State Diplomatic Security publish no protectee-specific threat counts, so those communities are read through individual incidents. Some Department of Homeland Security assault-increase percentages are agency-asserted and not independently corroborated. We cite the mechanism and leave the percentages out. Doppel surface shares are averaged per customer across customers that monitor social media, paid ads, and domains, so no single customer's volume sets the mix. They are not scoped to any single sector.

Findings are based on Doppel telemetry across a global customer base, with strongest coverage in North America. Public figures are attributed to their original source and are not Doppel findings.



Our mission is to protect the world from social engineering attacks every day. Our AI-native defense anticipates deception and eliminates threats.

1B+ INDICATORS ANALYZED DAILY

300+ TRUSTED CUSTOMERS

doppel.com

Prepared by Doppel SECR - Social Engineering Counterintelligence & Research

© Doppel Inc. 2026. All Rights Reserved.