carahsoft

Doppel

Today's Webinar

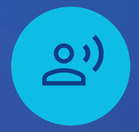
Federal Threat Intelligence Briefing: Defending Government Executives from AI-Driven Social Engineering

September 15, 2026

Thank you for joining us. The webinar will begin soon at 1:30pm Eastern; 10:30am Pacific.

For other events and training opportunities, visit: **carah.io/events**

Logistics



Sound

To hear today’s presentation, please turn on your device’s speakers.

Recording

Today’s session is being recorded. A copy of the recording will be sent to you via email within one business day.

Questions

Please use the Q&A function to ask questions throughout the presentation.

carahsoft

Doppel

About Carahsoft Technology Corp.

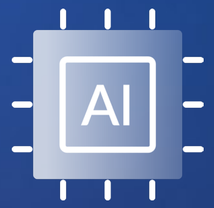
The Trusted Government IT Solutions Provider®

carahsoft.

Carahsoft connects customers with industry-leading technology solutions.

- Serves as the **Master Government Aggregator®**, connecting agencies, technology vendors and industry partners.
- Helps deliver **innovative, mission-focused solutions**.
- Supports organizations in **modernizing technology, strengthening operations and maintaining compliance.**
- Streamlines procurement through a wide variety of contract vehicles including **NASA SEWP V and more.**

Visit **carahsoft.com/solve** to explore our extensive technology portfolios with solutions for IT initiatives, including:



Artificial Intelligence

Cybersecurity

Emerging Technology

Legal & Courtroom Technology

Healthcare Technology

FinOps

Continuing Professional Education (CPE) Credit

*We are pleased to offer up to **1 CPE credit** for today's webinar.*

To qualify, you must:

1. Attend the live webinar
2. Stay actively engaged throughout the presentation
3. Answer the polling questions during the session

For more information on the CPE credits we are offering, our CPE sponsor (NASBA), and submission process, please visit our CPE information page: **https://carahevents.carahsoft.com/Event/Register/808415-cs5**

Today’s Speaker

Dylan DeAnda

Field Chief Technology Officer
Doppel

carahsoft

Doppel

Doppel

DOPPEL AND CARAHSOFT WEBINAR

Defending government executives and and agencies from AI-driven social engineering

TRADITIONAL PERIMETER

The new federal attack surface beyond the network.

Defending executives, agencies, and public trust from AI-enabled social enabled social engineering.

PRESENTED BY

Dylan DeAnda, Field CTO, Doppel
Doppel

HOSTED WITH

Carahsoft

What this briefing covers

01 **How the attacks start**

Social engineering as the entry method, and where impersonation of an individual actually appears.

02 **The attack chain**

Five repeatable stages, the channels that carry each one, and how the chain moves from online to from online to offline.

03 **Why identity is the protected surface**

The executive, the contact graph, and the agency seal as one identity problem.

04 **What a modern posture requires**

Four controls, sequenced, and how to measure whether they work.

PRESENTER

Dylan DeAnda

Field Chief Technology Officer, Doppel

U.S. Army Military Intelligence, signals intelligence analyst and Korean linguist.

Roughly 30 years in cybersecurity, including seven years leading federal and DoD programs.

EVIDENCE BASE

Public government reporting: FBI, IC3, U.S. Capitol Police, Police, U.S. Marshals Service.

Doppel telemetry: share of detections across a commercial customer base, strongest coverage in North America.

Observation and assessment are labelled separately throughout.

OPENING POLL · ENGAGEMENT CHECKPOINT 1 OF 4

Which best describes your primary responsibility?

Respond in the polling panel

CISO / CIO

Threat Intelligence

Physical Security

Public Affairs / Communications

SOC / Incident Response

Protective Intelligence / Executive Protection

Fraud

Other

Whatever the spread, one campaign will cross most of these columns before anyone escalates it.

LEARNING OBJECTIVES · CPE

What you will be able to do by the end of this session

01 Recognize how a digital threat aimed at one government executive becomes agency-level risk

02 Distinguish a coordinated campaign from an isolated indicator, using field evidence

03 Analyze impersonation activity as one campaign across five stages rather than as separate channel alerts

Four checkpoints run during the session: one opening poll and three CPE questions, each tied to one objective above.

Node counts are graph-clustered activity, not confirmed impersonations. Scenarios marked illustrative are not specific agency incidents.

Social engineering exploits trusted identities, not controls.

The attacker does not breach the network. They present a trusted identity on a channel the agency does not own, and ask an authorized person to act.

WHAT THE ENTERPRISE STACK OBSERVES

Network and endpoint	No event
Identity systems	No anomaly
Email controls	Never traversed

The activity occurs on external channels: social platforms, messaging apps, telephone, search and paid ads.

WHAT THE ATTACKER NEEDS

A credible identity
Name, title, portrait, voice, public by virtue of the role

A plausible pretext
A meeting, a verification step, a benefit, an urgent request

A channel outside the agency
Social, SMS, voice, then encrypted messaging

A small first request
A contact number, an introduction, a document, a payment

No security control was broken. Detection has to happen where the impersonation happens.

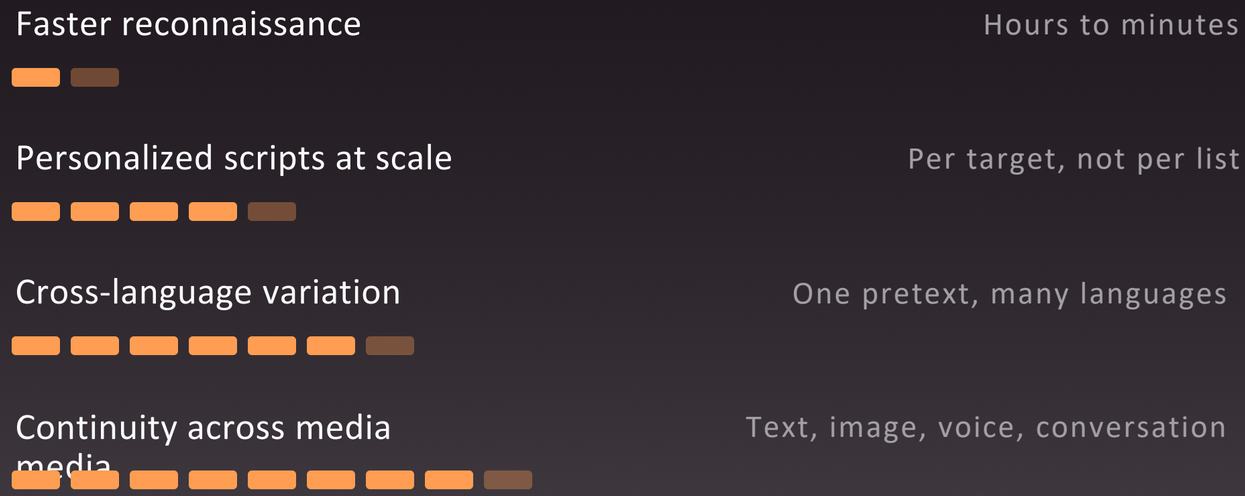
AI did not invent the con. It changed the economics.

Less time creating each approach. More time learning which approach works.

The operator's constraint used to be production. Now it is selection. Volume of credible attempts, not technical sophistication, is what reaches a trusted contact.

Not every campaign is AI-enabled, and the tooling is not is not autonomous. It compresses cost, speed, personalization, and language coverage.

FOUR OPERATIONAL CHANGES, AND HOW VARIATION COMPOUNDS



Relative and illustrative. Direction of change, not a measured multiple.

EXECUTIVE PROTECTION

The executive is rarely the entry point. The relationship ring is.

THE ADVERSARY PATH, AND NONE OF IT TOUCHES AN AGENCY SYSTEM

A Buy the government executive's address and household detail from people-search brokers.

B Clone the voice and display name from public role public role material.

C Reach staff, family, or peers, then move them to an them to an encrypted channel.

THE RELATIONSHIP	WHAT IT CARRIES TO THE ATTACKER
Chief of staff	Authority and confirmation
Scheduler	Calendar and urgency
Family and household	Residence and routine
Peers and contractors	Mission access and funds
Public and media	Belief in official guidance

WHY THIS MATTERS

Monitor impersonation of these identities and give them a verification verification protocol.

This does not mean monitoring the people themselves. No unrestricted monitoring of family or private communications.

Two identities are impersonated. The executive and the seal.

Anonymized exposure review review

IDENTITY ONE

The Executive

Name, title, likeness, and voice. Borrowed to make an approach believable to peers and staff.

IDENTITY TWO

The agency itself

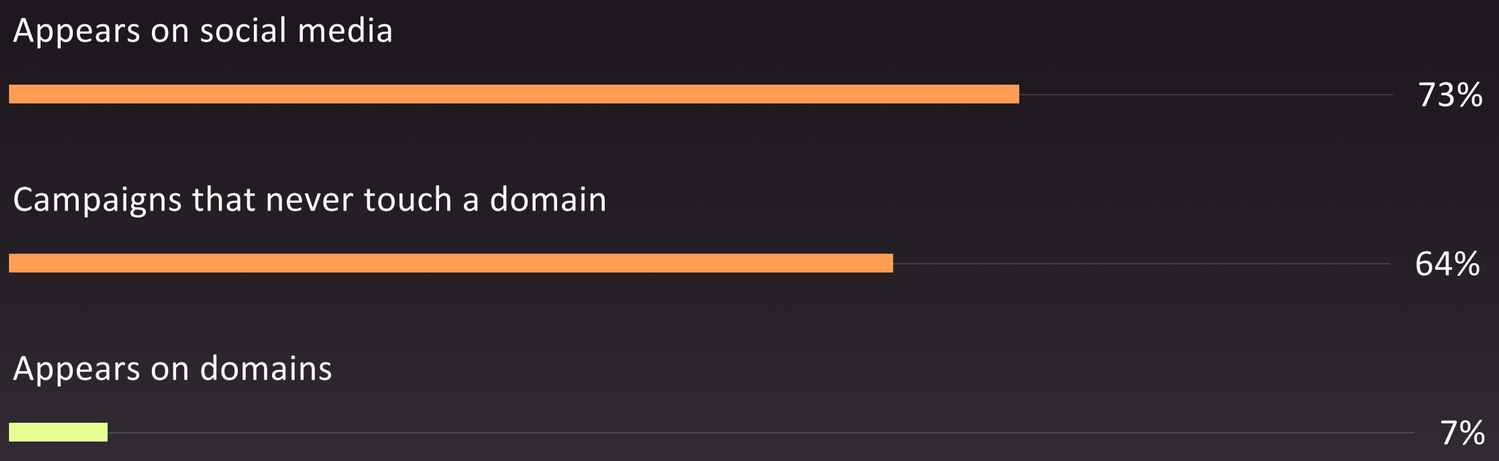
Seal, component names, official forms, mobile apps, apps, and the language of a government notice. notice. Borrowed to make a process look legitimate. legitimate. One campaign usually needs both.

WHERE THE SEAL TURNED UP, IN ONE DEPARTMENT'S EXPOSURE REVIEW

Domains	Government-style naming and cloned official content
Social	Department, component, and executive identities on six platforms platforms
Apps	Official mobile apps on unofficial APK platforms
Paid ads	Enforcement-themed advertising to audiences seeking urgent help
E-commerce	Seals, badges, and editable government-themed templates
Crypto	Token listings clustered on a single launch platform

Doppel external exposure review of a cabinet-level federal department, Sep 2026. Anonymized, shared with approval.

Impersonation of a person does not live on domains



Impersonation of an organization splits far more evenly across surfaces. The executive case is lopsided, which is what makes a domain-first posture misleading for a government executive.

PUBLIC FIGURES, FOR CONTEXT

Gov-impersonation losses, 2024 to to 2025	+97%
Threats to Congress, 2025	14,938
Threats to federal judges, FY2025	564

FBI IC3 · U.S. Capitol Police · U.S. Marshals Service

Doppel telemetry is reported as share of detections, aggregated across a commercial customer base with strongest coverage in North America. Public figures are attributed to their original source and are not Doppel findings.

PUBLIC GOVERNMENT REPORTING

The measured scale, from three federal sources.

CITIZEN LOSS

$797.9M

Government-impersonation losses in 2025, up 97 percent from $405.6M

Victim-reported loss from counterfeit federal authority: fake benefit, refund, and enrollment schemes.

FBI IC3 annual reporting

Does not prove prevalence of executive targeting.

LEGISLATIVE BRANCH

14,938

Threats against Members of Congress logged in 2025, a record and up 58 percent

Protective programs already carry the volume. These are recorded threats, not campaigns.

U.S. Capitol Police

The lighter bar is implied from the stated increase, not a published figure.

JUDICIARY

564

Threats against federal judges tracked in FY2025, with a further increase projected

The judiciary shows the clearest full chain from from online exposure to physical incident.

U.S. Marshals Service

No prior-year figure is published, so no comparison is drawn.

WHY THIS MATTERS

Volume and consequence are both rising. Attribution is a separate question.

These figures do not establish that a given threat was AI-enabled, or that any belong to one campaign. Public figures are attributed to their original source and are not Doppel findings.

THE SOCIAL ENGINEERING ATTACK CHAIN

Five stages, carried by different channels. One channel shows you one stage.

CHANNEL THAT CARRIES IT	01 Setup	02 Launch	03 Contact	04 Engagement	05 Compromise
Domains	●	●	·	·	·
Email	●	·	·	·	·
Social	·	●	●	·	·
Paid ads	·	●	·	·	·
Telco, voice and SMS	·	·	●	·	·
Messaging	·	·	●	·	·
Encrypted messaging	·	·	·	●	·
Observable to an agency	Yes	Yes	Yes	No	No

A domain-only view can be closing stage one while the campaign is already at stage three. Stages four and five are inferred from what the pages collect.

64%

of coordinated campaigns never touch a domain at all. Doppel telemetry, share of detections

CAMPAIGN CORRELATION

One operator, one identity, many artifacts.

THE SEED

A public role identity

Name, title, official portrait, biography, and recorded voice, all public by virtue of the office.

Cloning it requires no access to any agency system.

ARTIFACTS PRODUCED BY ONE CAMPAIGN

Two of the nine are visible to domain tooling. Seven are not.

- Lookalike domains — Seen by domain tools
- Spoofed mailboxes — Seen by domain tools
- Fake social profiles — Outside that view
- Messaging account — Outside that view
- Cloned voice — Outside that view
- Synthetic video — Outside that view
- Paid ads — Outside that view
- Broker-sourced data — Outside that view
- Doxxing page — Outside that view

WHY THIS MATTERS

Two artifacts removed, seven left operating. Correlation moves the unit of defense from the artifact to the campaign.

Composite of artifact types observed in Doppel case work, not a single named case.

ONLINE TO OFFLINE

One chain, then a fork: information and access, or physical harm.

Step 01

Reconnaissance and PII collection

Public role material plus broker records: addresses, household detail, staff and family relationships.

Step 02

Impersonation and deception

Cloned profiles, spoofed display names, cloned cloned voice, and synthetic media carrying the the executive’s identity.

Step 03

Contact on an encrypted channel

Staff, peers, family, or the public are moved to to Signal, Telegram, or WhatsApp, where the ask is ask is made.

THE CHAIN FORKS

INFORMATION AND ACCESS TRACK

- Credential theft and account access
- Payment and procurement fraud
- Information collection and foreign intelligence value

PHYSICAL-HARM TRACK

- Doxxing and incitement using brokered addresses
- Swatting and harassment at the residence
- Physical incident at home or in transit

WHY THIS MATTERS

The online warning signs come first. That makes them part of the of the protective picture.

The 2020 attack on a federal judge’s family home, after her address was was assembled from public and brokered sources, remains the reference reference case.

CPE QUESTION 1 OF 3 · ENGAGEMENT CHECKPOINT 2 OF 4

Respond in the polling panel.
Answer reviewed live.

Which scenario best demonstrates how a digital threat threat targeting a government executive can create broader agency-level risk?

A An executive receives an unsolicited commercial email

B A fraudulent executive account distributes false emergency guidance, directs users to a spoofed agency domain, and exposes the exposes the executive’s location

C An executive’s official biography appears on the agency website
website

D A constituent criticizes an executive’s policy decision online

The reference case: a home address, assembled from public records.

Step one

A public role

Name, court, official biography, and photograph, all public by virtue of the office.

Step two

The assembly

The residential address is compiled from public filings and and commercial data-broker records. No system is breached. breached.

Step three

The approach

The attacker travels to the family family home and presents as a a delivery.

Step four

The outcome

A fatal attack at the residence in residence in 2020. The judge’s judge’s son was killed and her her husband was wounded.

Step five

After

Official-privacy statutes followed, followed, creating a legal lever to lever to compel removal of judicial officers’ addresses.

THE OBSERVABLE WINDOW

Steps one through three ran on channels an agency can watch. Only step four was not observable.

WHY THIS MATTERS

Personal data is cheap to acquire and slow to remove, which is why exposure is a protective control and not a privacy nicety.

564

Judicial threats logged in FY2025. U.S. Marshals Service, via Doppel SECR-51

TREND TWO · THE SAME CHAIN, FOUR COMMUNITIES

One chain, four shapes, depending on who is protected.

Judiciary

Broker-sourced addresses to doxxing to swatting, and in 2020 a fatal attack at a judge’s family home. The clearest end-to-end chain on record.

564

Threats logged in FY2025, with a further increase projected. U.S. Marshals Service

Immigration enforcement

The sharpest 2025 surge in doxxing and online-to-offline threats, including a purpose-built built site assembled to publish publish personnel details. Doxxing Doxxing as infrastructure, not as a as a post.

Trend read from incidents rather than a published time series

Senior military executives

The likeness of one retired four-four-star officer, cloned into hundreds of fake accounts that that persist for years and are used used to run romance and investment fraud. The officer is is the bait; the citizen is the victim. victim.

Impersonation at scale. Attribution frequently unresolved

Members of Congress

The highest raw volume of any any protective community, and and the fastest growth in it.

14,938

Threat assessments in 2025, a a record and up 58 percent. U.S. U.S. Capitol Police

Executive-branch protectees face the physical end directly, including two 2024 assassination attempts and a 2026 checkpoint shooting near senior officials.

Each square is 1,000 logged threats, the same scale in both columns. Counting methods and populations differ.

U.S. Marshals Service, U.S. Capitol Police, and public reporting, via Doppel SECR-51

What one cabinet-level department’s exposure looked like across seven surfaces

■■■■■■■ Seven surfaces, all seven active, one department, one review

SURFACE	SCALE IN THE REVIEW	WHAT THE REVIEW FOUND
Domains	active, not counted	Government-style naming, cloned official content, clustered hosting
Social	■■■■■■ platforms	Agency impersonation across six platforms, concentrated on one
Executive protection	largest cluster in the review	Senior executives’ names and titles, several accounts per identity
Apps	active, not counted counted	Official agency apps repackaged on unofficial download platforms
Paid ads	active, not counted counted	Enforcement themes used as high-engagement hooks
E-commerce	active, not counted counted	Seals, badges, and editable government document templates, for sale
Crypto	active, not counted counted	Token listings clustered on a single launch platform

WHY THIS MATTERS

No single team inside that department owned more than one of these rows.

Every surface was active. Only the largest cluster was counted in the review, so the rest carry no number.

Client-confidential source, anonymized. Do not present externally without written customer approval. Observations are as reported and are not attributed to any actor.

CPE QUESTION 2 OF 3 · ENGAGEMENT CHECKPOINT 3 OF 4

Respond in the polling panel.
Answer reviewed live.

Which finding most strongly indicates a coordinated attack campaign rather than an isolated indicator?

A A single negative social-media post mentioning an agency executive

B One misspelled reference to an executive in an online forum

C Multiple impersonation accounts, look-alike domains, shared infrastructure, and coordinated messages targeting the executive and executive and agency across several channels

D A legitimate news article linking to the executive’s official biography

CASE THREE · DOPPEL SECR-175, OBSERVED 06 06 JAN TO 26 AUG 2026

Attack chain 01 Setup 02 Launch 03 Contact 04 Engagement 05 Compromise

One impersonation alert expanded into a multi-surface citizen-fraud network

ONE DOT PER CONNECTED NODE · 1 flagged balance-check page · 37 confirmed impersonations actioned · 219 connected nodes in total

7 brands hit by one reused kit **4** channels in the network

Almost none of the connected infrastructure had been reported independently.

WHAT DOPPEL INDEXED, STAGE BY STAGE

Stage 1 · Setup

Lookalike domains and spoofed support mailboxes registered

Stage 2 · Launch

Fake balance-check and refund refund pages plus agency-named social accounts

Stage 3 · Contact

Victims routed to the pages pages from search and social social

Stage 4 · Engagement

Victim interaction occurs off off indexed surfaces

Stage 5 · Compromise

Card and credential capture inferred from the collection forms

WHY THIS MATTERS · FEDERAL READ-ACROSS

Fake FEMA disaster-assistance portals, USCIS service sites, and TSA PreCheck enrollment pages pair a trusted government identity with a fee or verification step and a form that harvests payment and personal data. A citizen who reaches one fake page is usually one search result from the same operator’s other domains and support numbers.

High confidence this is one operation. Node count is clustered activity, not confirmed impersonations.

The conversation moves to Telegram. So does the evidence.

WHERE IT GOES

Public channel →

- Telegram
- Signal
- WhatsApp

Cloned voice and spoofed name, then a move off channel.

FBI public service announcements, 2025

WHERE IT LIVED

Six platforms. The filled square is Telegram, which carried the largest share.

One department impersonated across six platforms.

Anonymized federal department exposure review, Sep 2026

WHAT TIED IT TOGETHER

- One Telegram handle
- One email address
- One WhatsApp number

198

nodes, one operation

One shared contact identity across a storefront and its mirror.

Doppel SECR-177, observed 18 Apr to 02 Sep 2026

WHY THIS MATTERS

The ask is made where nobody is watching, by an operator reusing one identity. Reuse is the link.

Doppel indexes the public side of messaging: handles, channels, listings. Not private conversations.

TELEGRAM FRAUD TAKEDOWN

Published benchmark, representative. Not a commitment or guarantee.

CPE QUESTION 3 OF 3 · ENGAGEMENT CHECKPOINT 4 OF 4

Respond in the polling panel.
Answer reviewed live.

An adversary uses exposed personal information to impersonate a senior official, contacts members of the official's staff using AI-generated voice, and directs them through a messaging app to a fraudulent domain. How should this activity be analyzed?

A As separate alerts organized by channel and assigned independently

B As a domain-abuse incident because the fraudulent website is the final destination

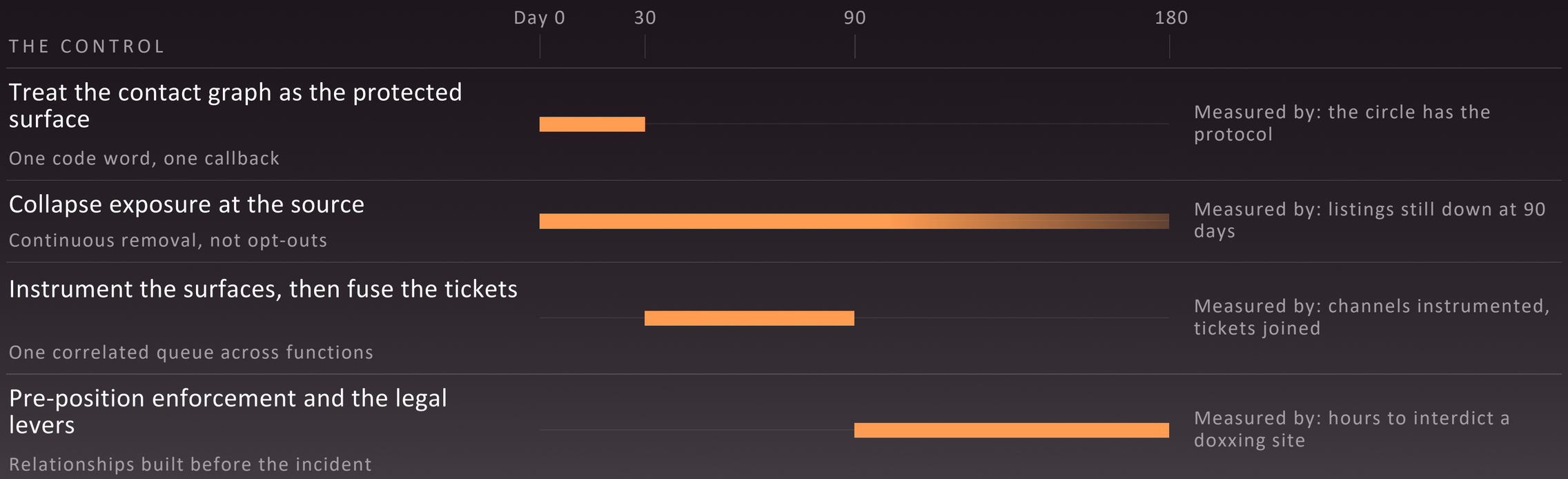
C As one coordinated campaign mapped across reconnaissance, persona development, impersonation, social engineering, and engineering, and attempted exploitation

D As an executive-protection matter only if a physical threat is identified

E Unsure

SECR-51 RECOMMENDATIONS

Four controls, in the order they can be executed.



WHY THIS MATTERS

None of the four requires a technology vendor to begin.

Source: Doppel SECR-51, Federal Executive Protection, section 05

MEASUREMENT

Detection is table stakes. Time to dismantle is the key metric.

WHAT A PROTECTIVE PROGRAM SHOULD MEASURE

Surface coverage	Channels instrumented, not domains watched
Correlation rate	Artifacts joined into one campaign record
Time to removal	From detection to provider action, per surface
Exposure kept down	Broker listings still absent after 90 days

All four are answerable inside an agency and do not depend on any single vendor.

DOPPEL PUBLISHED BENCHMARKS

Under 10 hrs

Median takedown across domains, social, and paid ads

~12 min

Median phishing-URL mitigation

Weeks to days

Telegram-fraud takedown compared with legacy process, representative

Published benchmarks, not commitments or guarantees. guarantees. Provider action varies by evidence, policy, jurisdiction, and urgency.

Next steps for attending teams

FROM DOPPEL

The SECR-51 threat brief

Federal Executive Protection, TLP: CLEAR, with the full source list and caveats.

A campaign-correlation walkthrough

How one seed indicator expands into the connected network behind it, and what it, and what evidence is produced.

A protectee exposure review

Scoped to your government executives: live impersonation inventory, contact-contact-graph map, and broker footprint.

THROUGH CARAHSOFT

- Acquisition through existing contract vehicles.
- A bounded 30-day proof of value for a named protective protective detail.
- Deployment with no on-premise infrastructure required.

Scope, duration, and any performance language to be confirmed jointly with Carahsoft. No authorization or accreditation claim is made in this briefing.

Start by understanding which executives, which relationships, and which agencies are exposed today.

Doppel

QUESTIONS AND DISCUSSION

Three things to carry out of this briefing

01

Most attacks on federal executives begin with social engineering, not intrusion.

02

They follow a repeatable five-stage chain, and it is observable before the ask.

03

In executive protection, the identity and the contact graph are the protected surface.

PRESENTED BY

Dylan DeAnda, Field CTO, Doppel · hosted with Carahsoft

Appendix follows: provenance, coverage, and case detail

Doppel

THANK YOU

Two things you can take from this session

The SECR briefing

- Federal Executive Protection, TLP: CLEAR
- Full source list and every caveat in this deck
- Sent as a PDF, no meeting required

A custom External Threat Landscape report

- Scoped to your agency and your named executives
- Live impersonation inventory across every channel
- Contact-graph map and data-broker footprint per government executive executive

WHAT IT TAKES TO START

One email, and the list of executives you protect. Request either through through Carahsoft or in the chat panel.

Dylan DeAnda, Field CTO, Doppel · hosted with Carahsoft

Scope and duration confirmed jointly with Carahsoft. Carahsoft. No authorization or accreditation claim is claim is made.

Q & A

carahsoft

Doppel

QUESTION AND PROCUREMENT REFERENCE

Appendix

Denser reference layer. Eight slides: capability by loop step, channel coverage status, status, telemetry shares, two federal-relevant case reads, an anonymized exposure exposure review, community patterns, and sources with open dependencies.

PROCUREMENT REFERENCE

Isolated alerts, or campaign defense.

TRADITIONAL REACTIVE POSTURE	DOPPEL CAMPAIGN DISRUPTION
6 disconnected alerts	1 unified picture picture
Isolated tickets across separate domain, social, and endpoint monitoring tools.	Shared infrastructure, fake personas, and multi-channel content in a single operating operating view.
2 of 9 removed	Full network
Two lookalike domains come down. Social profiles, messaging channels, and ad lures ad lures keep operating.	Interdiction across social, domain, messaging, and data-broker surfaces together. together.
Elapsed weeks	Elapsed hours
Manual evidence gathering creates lag while adversaries re-register assets.	Agentic workflows dismantle the campaign network in hours.

WHY THIS MATTERS

Removing two artifacts is a metric. Constraining the campaign is an outcome.

Describes operating models, not a specific product evaluation. Published benchmarks, not commitments. Provider action varies by evidence, policy, and jurisdiction.

PROCUREMENT REFERENCE

Where the gap sits, surface by surface.

THREAT SURFACE OR VECTOR	LEGACY DOMAIN AND OSINT TOOLS	DOPPEL
Social media impersonation  73%	Manual reporting, reactive tickets	Automated multi-platform disruption
Domainless campaigns  64%	Completely blind	Correlated asset and persona graph
AI voice and contact fraud	No native protection	Contact-graph verification and correlation
Data-broker and doxxing removal	One-time manual opt-outs	Continuous automated suppression
Mitigation speed	Weeks per isolated item	Hours for the campaign network

WHY THIS MATTERS

The two surfaces carrying most of the activity are the two a domain-first program cannot reach.

Shares are Doppel telemetry, share of detections. Comparison describes operating models, not a specific product evaluation.

APPENDIX A3

The difference sits in the loop, not the detection

LOOP STEP	DOMAIN AND OSINT POSTURE	DOPPEL
See it	Domains and mailboxes, plus manual platform search	Instrumented across domains, social, messaging, apps, ads, and telco
Connect it	Separate tickets per artifact and per team	One campaign record joined by identity, infrastructure, timing, and content
Validate it	Analyst screenshots assembled per request	Evidence and provenance captured with source, timestamp, and confidence
Constrain it	One report per asset, one provider at a time	Coordinated action across the mapped network, with status tracked
Catch its return	Case closed on removal	Revival monitoring tied to the original campaign record

Comparison describes operating models, not a specific product evaluation. Provider action varies by evidence, policy, and jurisdiction.

Source: Doppel SECR-51 and Doppel product documentation

APPENDIX A4

Channel coverage is stated per surface, never implied

SURFACE	WHAT APPEARS THERE	STATUS
Domains	Lookalike registrations, cloned pages	Pending confirmation
Social	Impersonating profiles, channels, groups	Pending confirmation
Messaging	Handles and numbers used for buyer or victim contact	Pending confirmation
Telco	Support numbers reused across brands	Pending confirmation
Email	Spoofed support mailboxes	Pending confirmation
Apps	Repackaged or unofficial distribution of agency apps	Pending confirmation
Paid ads and search	Sponsored placements routing to fake pages	Pending confirmation
E-commerce and marketplaces	Insignia, templates, and document kits	Pending confirmation
Crypto	Token listings referencing agency identities	Pending confirmation
Dark web	Access and account resale offers	Pending confirmation

Placeholder statuses. Each cell must be set to current, partner-supported, roadmap, or not supported by product and legal before this slide is used externally. No externally. No private-channel access is implied.

The attacker sees one campaign. The agency sees separate queues.

SEVEN QUEUES, SEVEN FRAGMENTS

Email security security	One lookalike domain
Executive protection	A reported voice note
Threat intelligence	An unattributed indicator
Fraud	A payment-collection page
Public affairs	A fake official profile
Legal and privacy	A takedown request
Brand protection	A paid ad

Each function sees something valuable. The campaign crosses all of them.

ONE CORRELATED OPERATING PICTURE

The same seven artifacts, connected by what they share

- Identity and persona
- Shared infrastructure
- Timing
- Behavior and content
- Objective
- Evidence and provenance

In Doppel telemetry, 64% of coordinated campaigns never touch a domain at all, so a domain-first queue never opens a ticket.

Source: Doppel telemetry, share of detections, SECR-51

Connected evidence turns alerts into decisions.

WHAT THE DETAIL NEEDS ANSWERED

01 What is the attacker trying to accomplish?
1

02 Who else is being targeted?

03 Which infrastructure is reusable?

04 What evidence is required for action?

05 What is likely to appear next?

SIX OBJECTS, ONE CAMPAIGN RECORD

Lookalike domain
Registrar record · 12 Aug · high

Phone number
Telco alert · recurring · high

Official portrait, reused
Image match · 14 Aug · medium

Messaging handle
Public listing · 15 Aug · high

Paid advertisement
Ad library · 16 Aug · medium

Prior infrastructure
Prior case link · shared host · high

Every link carries source, timestamp, confidence, and owner. Attributes shown are illustrative.

219

Connected nodes from one flagged page

37 confirmed impersonations, 4 channels, one playbook against 7 brands · Doppel SECR-175, Jan to Aug 2026

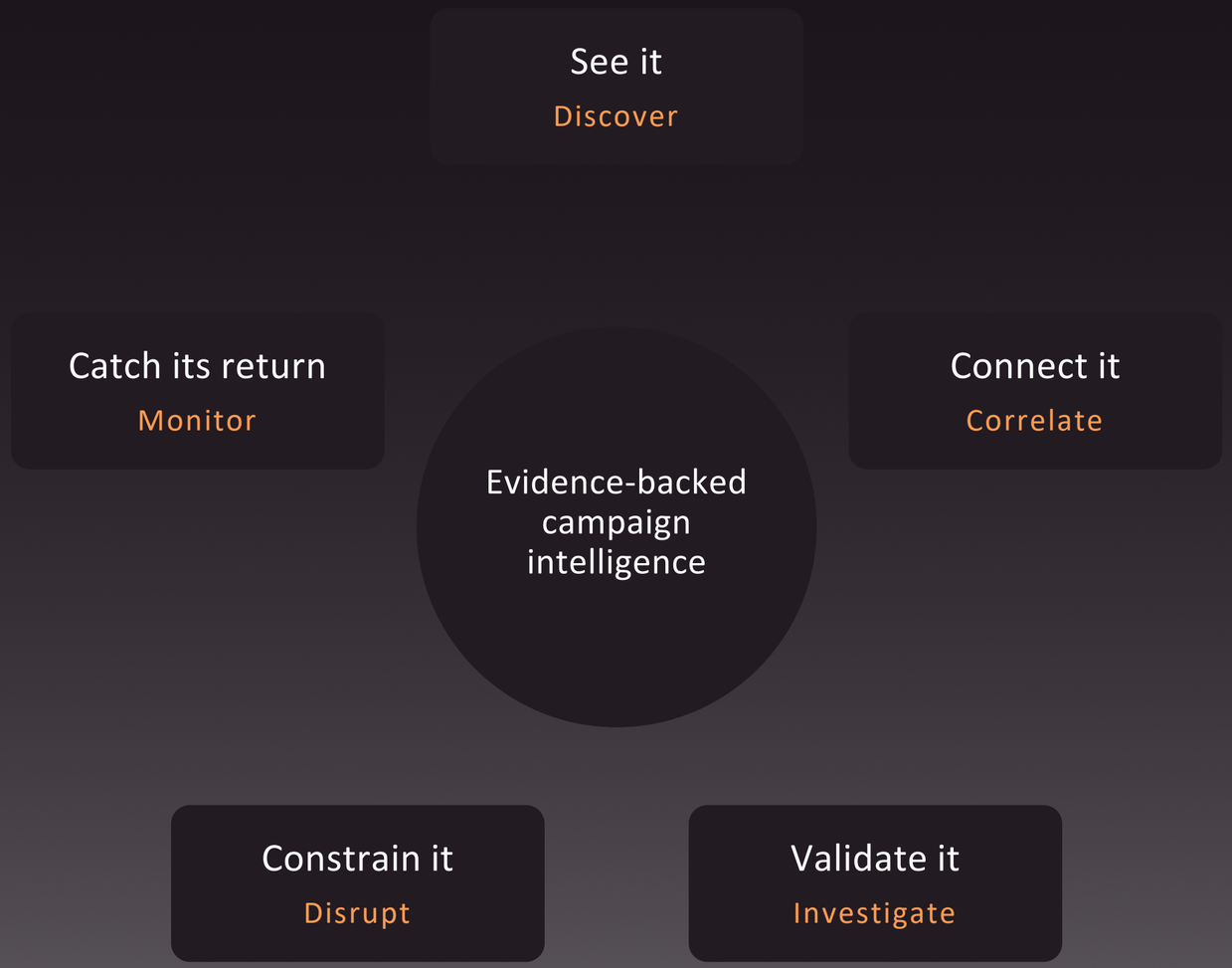
198

Connected nodes from one storefront listing

Linked by one recurring phone number, Telegram handle, and email · Doppel SECR-177, Apr to Sep 2026

Node counts are graph-clustered activity, a different measure from confirmed impersonations. Correlation is not attribution. Evidence and confidence remain explicit.

Doppel compresses discovery to disruption.



DIVISION OF LABOR

Technology provides scale, coverage, and consistency across surfaces.

Analysts provide judgment, context, escalation, escalation, and follow-through.

WHAT THIS DOES NOT CLAIM

No access to private channels. No autonomous attribution. No guaranteed or universal removal. Channel coverage is stated as current, partner-supported, or roadmap.

ASSESSMENT

Outlook: sustained elevated, through the next two quarters.

Identity-led, AI-accelerated, and online-to-offline. Impersonation, doxxing, and swatting are cheap, effective, and low-risk for the actor, which favors persistence. Direction is clear; magnitude is the open question.

AI IMPERSONATION

Rising

DOXXING AND PII EXPOSURE

Elevated

SWATTING

Elevated

PHYSICAL INCIDENTS

Episodic, severe

CAVEATS

Attribution for impersonation activity is frequently unresolved. Observation and assessment are separated separated throughout.

The U.S. Secret Service and State Diplomatic Security publish publish no protectee-specific threat counts, so those communities are read through incidents rather than a time a time series.

Some Department of Homeland Security assault-increase increase percentages are agency-asserted and not independently corroborated. We rely on the mechanism, not mechanism, not the multiples.

Doppel telemetry is measured as share of detections and is and is not scoped to any single sector or customer.

Source: Doppel SECR-51, section 06. Reporting window January 2024 to July 2026

The same pattern, five different shapes

COMMUNITY	HOW THE CHAIN EXPRESSES
Judiciary	The clearest full chain, from broker-sourced addresses to doxxing and swatting, and in the landmark 2020 case a fatal home attack. 564 threats logged in FY2025, with a further increase projected for 2026.
Immigration enforcement	The sharpest 2025 surge in doxxing and online-to-offline threats, including a purpose-built site publishing personnel publishing personnel details.
Senior military executives	Impersonated at scale for fraud. The likeness of a single retired four-star officer has been cloned into hundreds of hundreds of fake accounts that persist for years.
Members of Congress	The highest raw volume of threats, 14,938 logged in 2025, a record and up 58%.
Executive-branch protectees	Face the physical end directly, including two 2024 assassination attempts and a 2026 checkpoint shooting near senior officials.

Sources: U.S. Marshals Service, U.S. Capitol Police, public reporting, compiled in Doppel SECR-51

Protective communities without published protectee-specific counts are read through incidents, not a time series. Attribution for impersonation activity is frequently activity is frequently unresolved.

Federal authority is operational infrastructure.

The attacker does not need to steal the identity.
They need to borrow the authority attached to it.

THE CONVERSION

Identity + trusted role + credible channel

= operational action

FIVE MINUTES OF BELIEF

AUTHORITY RELATIONSHIPS THE CAMPAIGN BORROWS

Official to employee
Approve, transfer, disclose

Commander to subordinate
Comply without verifying

Agency to citizen
Pay a fee, submit records

Executive to contractor
Share access, move channel

Help desk to user
Reset, enroll, bypass

Executive to foreign counterpart
Open a private channel

An alert is not an outcome.

01	02	03	04	05	06	07	08
Detect	Validate	Preserve	Choose pathway	Act	Escalate	Verify	Monitor revival

ALERT		OPERATIONAL OUTCOME
Suspicious domain found	→	Abuse validated and evidence preserved
Fake account identified	→	Provider action initiated and tracked
Voice message reported	→	Related infrastructure and targets connected
Asset removed	→	Replacement infrastructure detected
Indicator counted	→	Campaign capacity constrained

The mission is not to count malicious assets. It is to reduce the campaign's ability to operate.

Provider action varies by evidence, policy, jurisdiction, urgency, and provider response. No universal removal guarantee is implied.

One campaign needs one operating picture.

One campaign owner. Federated execution. Shared evidence.

SHARED OUTPUTS

- ✓ Common campaign record
- ✓ Evidence and provenance
- ✓ Named owner
- ✓ Escalation path
- ✓ Action status
- ✓ Revival monitoring

An organizing model for functions that already exist. It exist. It does not require a new permanent organization, headcount, or reporting line.

A verified-account marketplace feeding transnational fraud

ONE DOT PER CONNECTED NODE

1 flagged product listing 6 confirmed impersonations 198 connected nodes in total

20+ crypto, banking, and payment platforms offered as pre-verified accounts

WHY THIS MATTERS TO AN INVESTIGATOR

Pre-verified accounts on exchanges, neobanks, and payment platforms are the cash-out and mule accounts that let fraud proceeds move without tripping identity checks. One storefront supplies many downstream operations, so mapping the storefront, its mirrors, its contact identity, and the platforms it services turns a single flagged page into account-resale infrastructure behind many cases.

THE CONNECTIVE SIGNAL

- One phone number recurring across several several unrelated monitoring programs
- A single Telegram handle carrying buyer contact contact
- One operator email address across listings
- A storefront mirror host used for staging

High confidence this is a verified-account marketplace. Lower confidence on its scale: the node count includes suspected and benign entities.

Thank You for Attending

Questions? Connect with us:

carahsoft

Cary White

Doppel Team | Carahsoft Technology Corp.

703-230-7507

Cary.White@Carahsoft.com

carahsoft.com/doppel

Doppel