# Emergency Directive 19-01

January 22, 2019

## Mitigate DNS Infrastructure Tampering

This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's Emergency Directive 19-01, "*Mitigate DNS Infrastructure Tampering*".

*Section 3553(h) of title 44, U.S. Code, authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to "issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise*

*maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat." 44 U.S.C. § 3553(h)(1)–(2)*

*Section 2205(3) of the Homeland Security Act of 2002, as amended, delegates this authority to the Director of the Cybersecurity and Infrastructure Security Agency. 6 U.S.C. § 655(3).*

*Federal agencies are required to comply with these directives. 44 U.S.C. § 3554 (a)(1)(B)(v)*

*These directives do not apply to statutorily-defined "national security systems" nor to systems operated by the Department of Defense or the Intelligence Community. 44 U.S.C. § 3553(d), (e)(2), (e)(3), (h)(1)(B).*

## Background

In coordination with government and industry partners, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is tracking a series of incidents[1] involving Domain Name System (DNS) infrastructure tampering. CISA is aware of multiple executive branch agency domains that were impacted by the tampering campaign and has notified the agencies that maintain them.

Using the following techniques, attackers have redirected and intercepted web and mail traffic, and could do so for other networked services.

1. The attacker begins by compromising user credentials, or obtaining them through alternate means, of an account that can make changes to DNS records.
2. Next, the attacker alters DNS records, like Address (A), Mail Exchanger (MX), or Name Server (NS) records, replacing the legitimate address of a service with an address the attacker controls. This enables them to direct user traffic to their own infrastructure for manipulation or inspection before passing it on to the legitimate service, should they choose. This creates a risk that persists beyond the period of traffic redirection.
3. Because the attacker can set DNS record values, they can also obtain valid encryption certificates for an organization's domain names. This allows the redirected traffic to be decrypted, exposing any user-submitted data. Since the certificate is valid for the domain, end users receive no error warnings.

To address the significant and imminent risks to agency information and information systems presented by this activity, this emergency directive requires the following near-term actions to mitigate risks from undiscovered tampering, enable agencies to prevent illegitimate DNS activity for their domains, and detect unauthorized certificates.

## Required Actions

### Action One: Audit DNS Records

- Within 10 business days, for all .gov or other agency-managed domains, audit public DNS records on all authoritative and secondary DNS servers to verify they resolve to the intended location. If any do not, report them to CISA.

*CISA recommends agencies prioritize NS records and those associated with key agency services offered to organizational users and the public (for example, websites that are central to the agency's mission, MX records, or other services with high utilization).*

### Action Two: Change DNS Account Passwords

- Within 10 business days, update the passwords for all accounts on systems that can make changes to your agency's DNS records.[2]

*CISA recommends the use of password managers to facilitate complex and unique passwords.*

**Action Three: Add Multi-Factor Authentication to DNS Accounts**

- Within 10 business days, implement multi-factor authentication (MFA) for all accounts on systems that can make changes to your agency's DNS records.[3] If MFA cannot be enabled, provide CISA with the names of systems, why it cannot be enabled within the required timeline, and when it could be enabled.

*CISA recommends using additional factors that are resilient to phishing. Consistent with NIST SP 800-63b, Short Message Service (SMS)-based MFA is not recommended.*

**Action Four: Monitor Certificate Transparency Logs**

- Within 10 business days, CISA will begin regular delivery of newly added certificates to Certificate Transparency (CT) logs for agency domains, via the Cyber Hygiene service.
- Upon receipt, agencies shall immediately begin monitoring CT log data for certificates issued that they did not request. If an agency confirms that a certificate was unauthorized, it must report the certificate to the issuing certificate authority and to CISA.

## CISA Actions

- CISA will provide technical assistance to agencies that report anomalous DNS records.
- CISA will review submissions from agencies that cannot implement MFA on DNS accounts within the timeline and contact agencies, as needed.
- CISA will provide regular delivery of newly added certificates to CT logs for agency domains via the Cyber Hygiene service.
- CISA will provide additional guidance to agencies through an Emergency Directive coordination call following the issuance of this directive, as well as through individual engagements upon request (through CyberLiaison).

**Reporting Procedures**

Agencies shall provide information to CISA per the schedule below:

- January 25, 2019: Submit Status Report
- February 5, 2019: Submit Completion Report for all actions detailed above

Beginning February 6, 2019, the CISA Director will engage Chief Information Officers (CIO) and/or Senior Agency Officials for Risk Management (SAORM) of agencies that have not completed required actions, as appropriate, to ensure their most critical federal information systems are adequately protected. By February 8, 2019, CISA will provide a report to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB) identifying agency status and outstanding issues.

**Duration**

This Emergency Directive remains in effect until replaced by a subsequent Binding Operational Directive or terminated through other appropriate action.

**Footnotes**

1. https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign ↩

2. This includes accounts on agency-managed DNS server software, systems that manage that software, third-party DNS operators' administration panels, and DNS registrar accounts (excluding the .gov registrar). ↩

3. Ibid. ↩

Return to top