VALIMAIL

TRUST YOUR EMAIL™

2020 ELECTION INFRASTRUCTURE REMAINS VULNERABLE TO EMAIL HACKING

VALIMAIL EMAIL AUTHENTICATION REPORT

OCTOBER 2020

EXECUTIVE SUMMARY

The United States is moving towards the November 3rd election facing a unique array of threats. Unfounded claims of election fraud and mail-in ballot tampering are rampant, while actual threats to the election infrastructure have gone mostly unaddressed.

Analysis of Domain Name System (DNS) records by Valimail finds that domains involved in the U.S. election remain vulnerable to the most pernicious form of email attack: Impersonation-based phishing. This means that most of these domains can easily be impersonated by attackers pretending to be a local election official, a state agency, a campaign, a political action committee, or even an election systems manufacturer.

This vulnerability may not be the largest challenge facing the 2020 election, but it is a significant indicator that best practices are not generally being followed. It's time for federal and state officials to prioritize Domain-based Message Authentication, Reporting, and Conformance (DMARC) enforcement for all domains involved in elections — including campaign-specific domains — to prevent mischief and outright disruption for the current and future elections.

INTRODUCTION

Valimail's analysis shows that, at virtually every level of the American election infrastructure, there is massive vulnerability to impersonation. This is due largely to the poor penetration of email authentication standards that can prevent spoofing.

Not only local governments, but also state governments, campaign and PAC domains, and election systems manufacturers are, by and large, unprotected from email spoofing. While this may not be the largest threat facing the 2020 election, it is cause for serious concern, as this is a widespread vulnerability that malicious agents could use to spread uncertainty, confusion, misinformation, and doubt — or even to affect the outcome of an election.

KEY FINDINGS

Only 15% of campaigns and political action committees (PACs) are protected from spoofing with DMARC enforcement

Democrats have better email security hygiene in this respect: Democrats.org is protected by DMARC enforcement; Donaldjtrump.com, GOP.com, and Joebiden.com are unprotected

Only 3.3% of U.S. state domains are protected

Just 7% of the largest counties' domains are protected — an increase of just 2 percentage points from 2019

Only one of the eight election systems manufacturers certified by the U.S. government is protected from email spoofing

Two specific email-based threats loom large: domain spoofing and phishing. These attacks can take multiple forms, from disinformation campaigns waged via mass mailings, to phishing attacks directed at campaigns or election officials, to attempts to hack into the email accounts of critical campaign officers or election managers.

There are standards in place to prevent this kind of spoofing. Domain-based Message Authentication, Reporting, and Conformance (DMARC), together with Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) provide robust protection against unauthorized senders sending email "from" a domain. These standards are utilized by nearly every major mail receiver in the world, representing about 80% of all inboxes globally. And they are increasingly widely deployed, with more than 1 million DMARC records deployed worldwide. Some industries — e.g. the Fortune 500 — are approaching or exceeding 50% penetration of DMARC usage, and 20% or greater protection through DMARC enforcement.

The phishing threats are not merely hypothetical. The 2016 Presidential election saw at least one successful case of a Russia-based threat actor, nicknamed "Fancy Bear," gaining access to the Democratic National Committee's mail system by means of a phishing email. In the 2018 midterm elections, phishing emails targeted many election officials in Southern states.

These attacks have intensified in the past year. In September, Microsoft researchers identified Fancy Bear as the perpetrator behind an attack on a consulting firm working with the Biden campaign.

In the same month, rural Hamilton County, Texas was the victim of a phishing campaign, in which an adversary sent official-seeming emails to the county clerk, purporting to contain voting results. The messages contained a malicious attachment, which then infected the clerk's office computers. ProPublica researchers stated that this attack was probably part of a broader campaign directed at many organizations, not just election officials — but added that "numerous smaller locales like Hamilton appear to have taken few precautionary measures."

DMARC POLICIES

DMARC allows domain owners to specify the policy that they would like email receivers to apply to any mail that appears to come from their domain but whose sender has not been authorized. Those policies are set via a "p=" tag in the DMARC record for that domain, which is published in DNS.

P=NONE

Monitoring Mode

Messages failing authentication are delivered normally

P=QUARANTINE

Quarantine Policy

Messages failing authentication should be sent to a spam or junk mail folder.

P=REJECT

Reject Policy

Messages failing authentication should be deleted outright.

If a domain has a correctly configured DMARC record with a policy at quarantine or reject, which is applied to 100% of email, and no exceptions for subdomains, it is said to be at "DMARC enforcement."

In September, Microsoft published details on three major operations targeting U.S. elections, from groups based in Russia, China, and Iran. At least one of these groups, nicknamed "Zirconium" by Microsoft, uses email as a primary attack vector, and is responsible for thousands of attacks against high-profile individuals associated with campaigns, resulting in at least 150 incidents of compromise.

Of course, email is not the only mode of attack. Cloudflare observed twice as many distributed denial-of-service (DDoS) attacks directed at political campaigns in April-June 2020, compared with the three previous months. And, the company also reported, "government election-related sites are experiencing more attempts to exploit security vulnerabilities," including more than 120,000 threats per day and almost 200 SQL injection attempts per day.

But email is uniquely vulnerable. It's ubiquitous. It's widely used for essential communications by campaigns, election officials, voting system manufacturers, and government officials. Email reaches half the planet's population, making it an indispensable marketing tool used by every political candidate, campaign, and party. And yet in its native state, email is highly vulnerable to attacks that leverage impersonation, malware, malicious links, and misinformation.

To understand the vulnerability of the U.S. election infrastructure to these kind of email attacks, Valimail examined the DNS entries for hundreds of domains relating to state and local governments, campaigns, and more, looking for DMARC and SPF records, and analyzing whether those records were correctly configured and what DMARC policy was in place for each one. We found, across the board, much lower than average rates of DMARC usage and DMARC enforcement policies. This is a shortcoming that should and could be remedied, if not before this election, certainly prior to the next major national election.

Our findings agree with the ProPublica report mentioned above, which focused on email systems used by city governments in swing states and found that "dozens of them relied on homebrew setups or didn't follow industry standards" including email authentication.

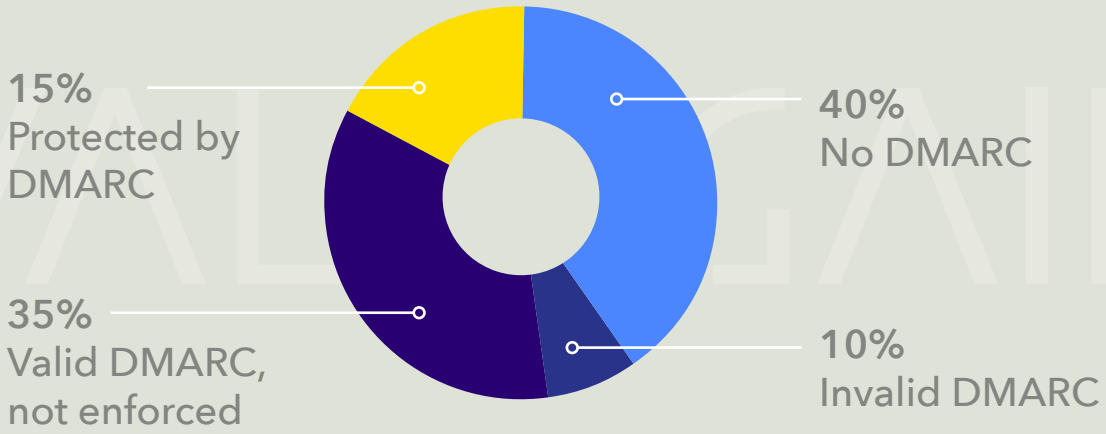
Fixing this vulnerability should be a priority now and for future elections.

TOP U.S. CAMPAIGNS AND PACS

How much can you trust that the political fundraising email really came from who it appears to come from — or that if you click the links in the message, that the money you donate will actually end up in the account of who you intended to support?

The answer, when it comes to most U.S. campaigns and political action committees (PACs), is simple: Not much.

CAMPAIGN AND PAC DOMAINS: DMARC ENFORCEMENT



SOURCE: VALIMAIL

We take a lot on faith when we open and click on emails sent by political campaigns and PACs. That's because, for the most part, the domains used by these organizations are not protected from spoofing through the industry-standard authentication technologies.

We'll start with the two leading presidential candidates. Joebiden.com is ostensibly protected by a DMARC record that is correctly configured and set to the most stringent policy, p=reject. As this report went into production, however, the domain's SPF record became misconfigured, exceeding the standard's built-in limitation of 10 DNS lookups (a technical constraint that domain owners often fail to observe).

However, Donaldjtrump.com is not protected. It has a correctly configured DMARC record, but the DMARC policy is p=none, meaning that spoofed messages impersonating this domain will be delivered as normal. Also, the SPF record associated with this domain has a misconfiguration that may result in authentication failures for some mail.

The candidates' parties have domains with similar configurations. GOP.com has a published DMARC record but a policy of p=none, while Democrats.org has a strict DMARC policy of p=reject. As a result, email from the Republican party can be more easily impersonated than email from the Democratic party.

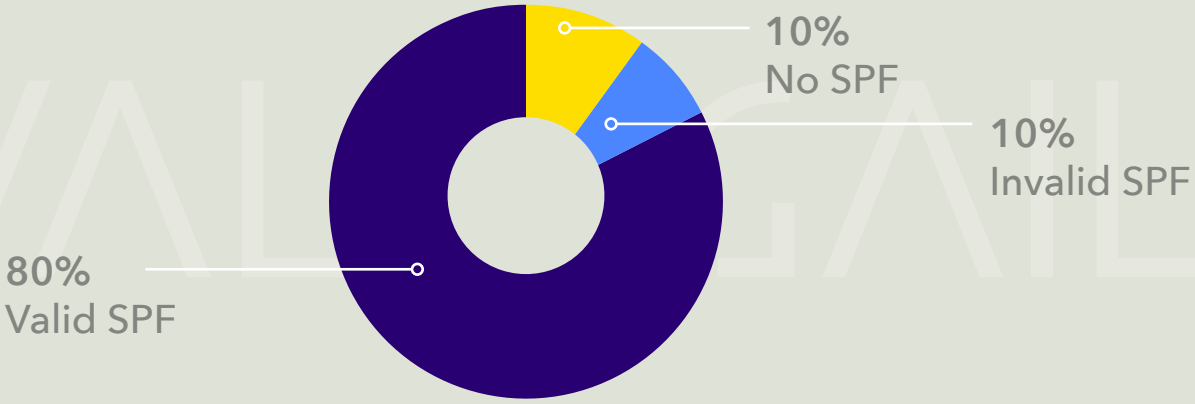
Examining these four domains together with domains for the 20 largest PACs and 20 largest SuperPACs, as listed by OpenSecrets.org, reveals that email security hygiene is not a high priority across the board. Of the 40 domains in this cohort, only 6, or 15%, are protected from spoofing with DMARC at enforcement (p=reject or p=quarantine policies). Domains with DMARC enforcement include three liberal-leaning PACs (emilyslist.org, lcv.org, and smart-union.org), one centrist organization (rtx.com, which is the domain of Raytheon, a major donor to both parties), and one conservative PAC (a1apac.org), in addition to the campaign domains mentioned above.

(There are only 40 domains for a total of 44 organizations because some of the PACs and SuperPACs do not have registered domains that we could find.)

Another 35% have DMARC records that are correctly configured but have a monitor-only policy (p=none), while 40% have not many any attempt to deploy DMARC at all.

Looking at SPF, which is an older and more widely deployed standard, we see that most of these campaigns and PACs have at least made the attempt to use SPF, with only 10% having no SPF record, and 82.5% publishing a valid SPF record.

CAMPAIGN AND PAC DOMAINS: SPF USAGE



SOURCE: VALIMAIL

This is not surprising for marketing-driven organizations, as SPF is a widely understood marketing best practice, which, if properly configured, can help improve the deliverability of emails sent from that domain. Unfortunately, SPF by itself provides no protection against impersonation, so domains with SPF but not DMARC (or with a DMARC policy of "none") can still easily be spoofed by malicious actors or spammers seeking to impersonate them.

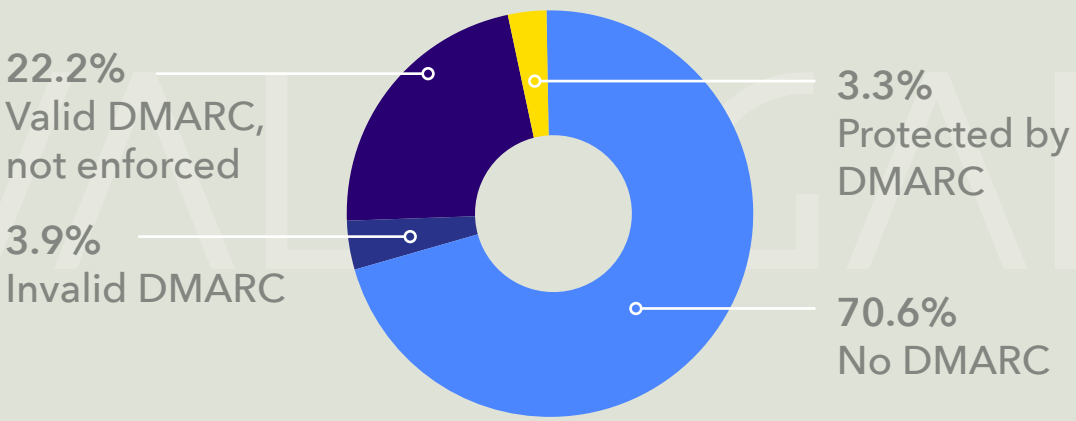
U.S. STATE DOMAINS

To get a bird's-eye view of the state of email security leading up to the election, Valimail examined a set of 153 domains owned by U.S. states, including .gov and .us variants of state names and two-letter state abbreviations (newjersey.gov, ca.gov, oh.us, and so forth).

These domains represent state governments at their highest levels, and in addition, are sometimes used (via subdomains) for county and local services. While these don't exhaust the universe of state-owned domains, this list is a good proxy for how well states are doing to protect their "digital brands."

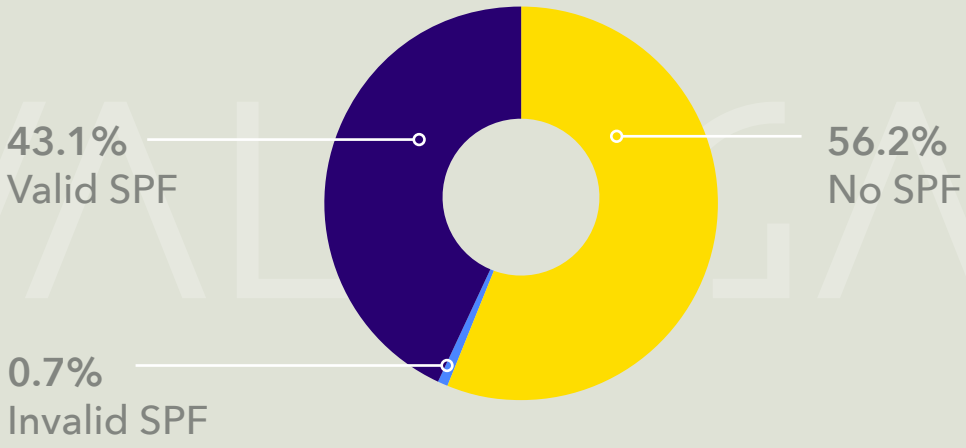
Valimail analysis shows that these states are, in general, not doing much to protect their brands. Only 5 of these domains, or 3.3%, are protected from spoofing by DMARC that is correctly configured, and set to an enforcement policy (p=reject or p=quarantine): nj.gov, alabama.gov, wv.gov, missouri.gov, and al.gov.

U.S. STATE DOMAINS: DMARC ENFORCEMENT



SOURCE: VALIMAIL

U.S. STATE DOMAINS: SPF USAGE



SOURCE: VALIMAIL

Another 34 domains (22.2%) have valid DMARC records but are not configured with an enforcement policy — they have policies in "monitor mode," or p=none, which means that spoofed messages that appear to come from that domain are still likely to be delivered as normal.

Another 6 domains (3.9%) have DMARC records that are incorrectly configured. And the vast majority, 108 domains (70.6%) lack DMARC altogether.

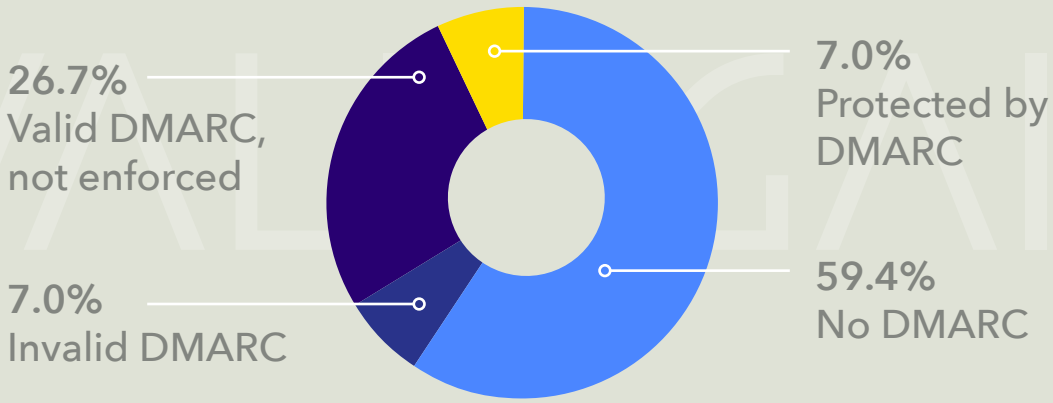
While state governments often follow the federal government's lead in deploying security technology, this is not the case here. Nearly 80% of federal government domains are protected by DMARC at enforcement, thanks to a 2017 order from the Department of Homeland Security mandating this technology.

(One notable exception: Whitehouse.gov is still unprotected.) State governments have not yet prioritized this aspect of email security.

State domains also have a low rate of SPF usage. This older, better-understood standard is a widely understood marketing best practice, as it can help improve email deliverability. But as state governments are not marketing-driven organizations, it's not surprising that penetration of this technology is shallower here.

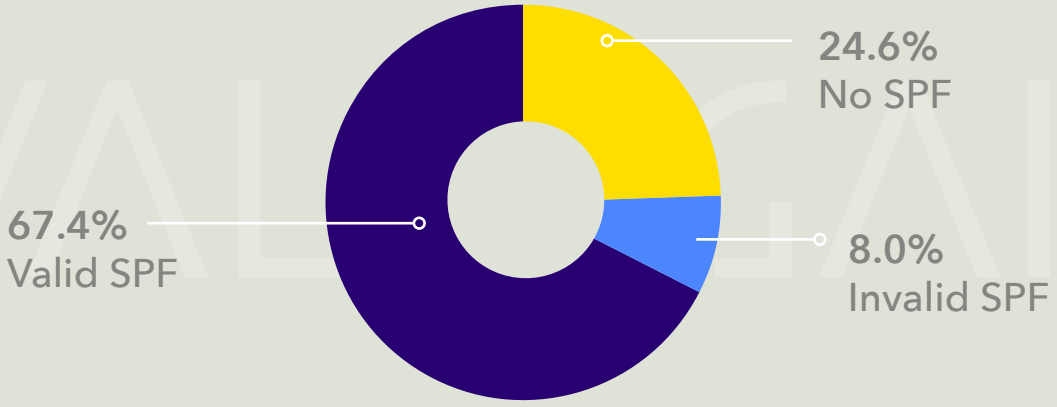
The impact of this security oversight on the U.S. election is uncertain. In the U.S., most elections are administered at the local level, so state domains have a limited role to play in the election.

BIGGEST U.S. COUNTIES: DMARC ENFORCEMENT



SOURCE: VALIMAIL

BIGGEST U.S. COUNTIES: SPF USAGE



SOURCE: VALIMAIL

However, it's not inconceivable to imagine a disinformation campaign aimed at suppressing voter turnout or sowing uncertainty about election results that utilized a state-owned domain. For example, an adversary might impersonate a message from a state government's secretary of state, declaring that a certain candidate had won that state. For that reason, the vulnerability of these domains to being spoofed is a concern.

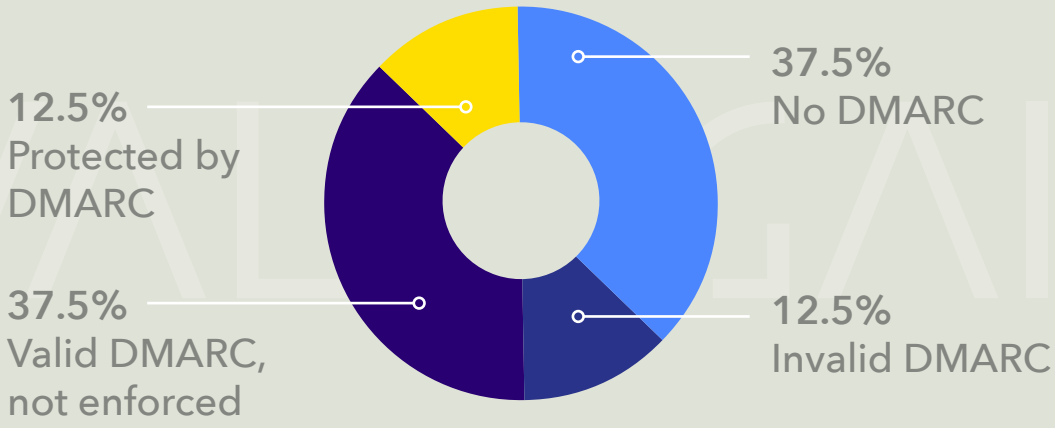
ELECTION SYSTEM MANUFACTURERS AND U.S. COUNTIES

U.S. elections happen largely at the local level, with elections administered by local boards of elections or registrars of voters. Those elections are usually conducted with voting and tabulation equipment sourced from a small number of manufacturers whose technologies have been vetted and approved by the Election Assistance Commission.

To check the email security of these organizations, Valimail compiled two lists. One represents domains used by the three most populous counties in every state, a list of 187 domains that we last examined almost a year ago, noting that email security remains a weak link in election infrastructure. The second is a list of domains used by the eight election systems manufacturers approved by the EAC.

For the top counties in the U.S., the picture is only slightly better than we found in 2019. Today, 7% of the country's largest counties are protected by DMARC that is properly configured and set to an enforcement policy of p=reject or p=quarantine, up from 5% in December 2019. Almost 27% have DMARC records but have set them to an unenforced, p=none policy, which does nothing to stop email impersonating them from being delivered. And the rest, 111 counties — 59.4% of the total — have no DMARC records at all.

ELECTION SYSTEM MANUFACTURERS: DMARC ENFORCEMENT



SOURCE: VALIMAIL

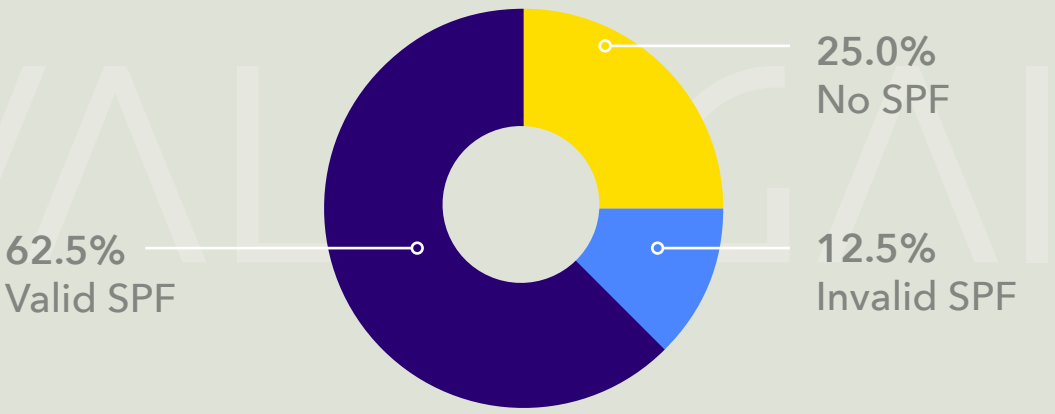
SPF usage among these counties is at a higher level than among state domains, perhaps reflecting the fact that these domains are more heavily used for sending email to local citizens. 67.4% of these domains have valid SPF records, and 24.6% have no SPF at all. Having a valid SPF record published in DNS can help improve deliverability of the emails a domain does send, but it does nothing on its own to protect the domain from being spoofed by imposters.

This lack of protection by DMARC is cause for concern, because it means that the vast majority of America's largest counties can easily be impersonated by spammers or bad actors. Bogus voter registration notifications, impersonated communications from boards of elections, faked announcements of voting results — all are possibilities that could be executed by a careful adversary, leveraging the implicit trust people are likely to place in a message that appears to come from an official domain.

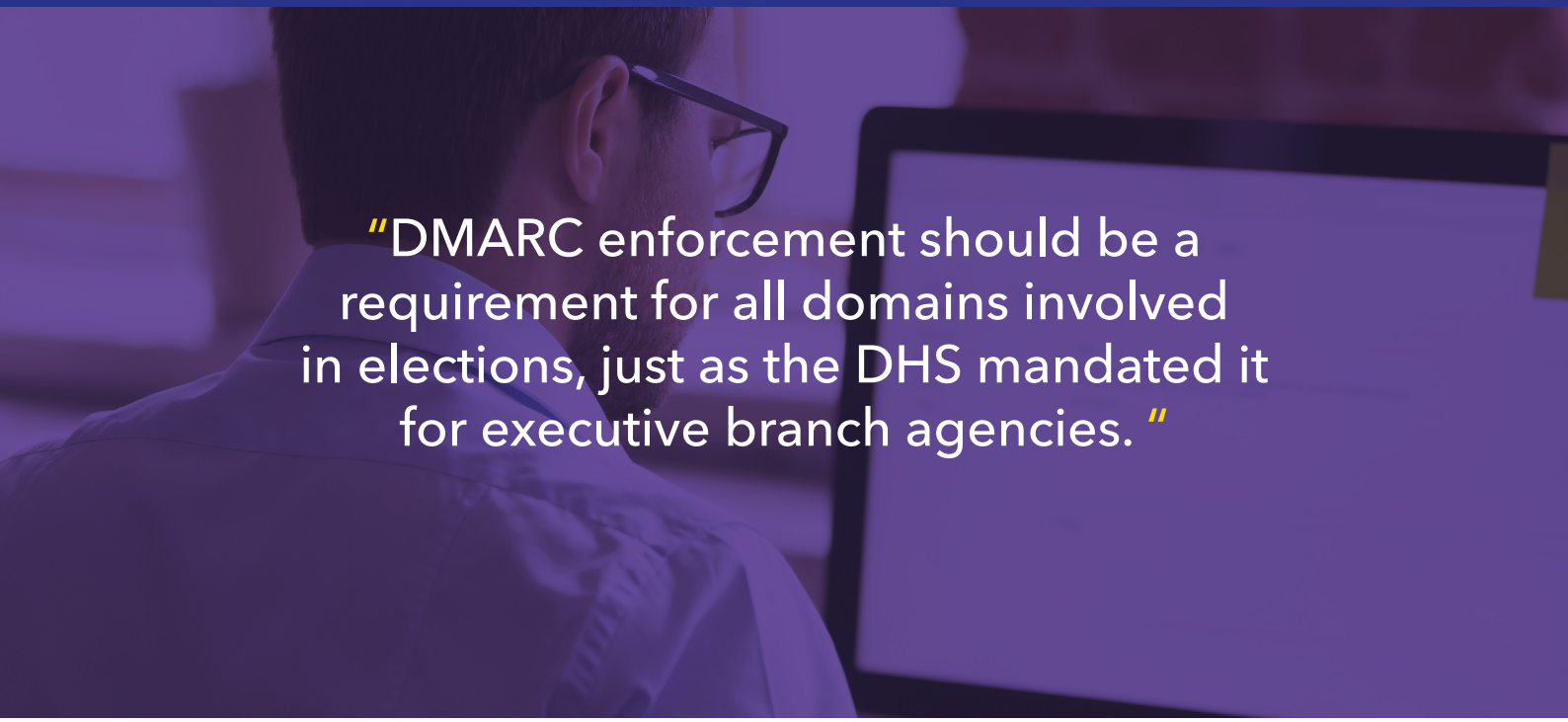
There is also cause for concern among the manufacturers of election equipment used throughout the country. Only one manufacturer, Smartmatic, has a domain that is protected from impersonation with a correctly configured DMARC record at enforcement. The rest can easily be spoofed.

Penetration of SPF is higher, with five domains having correctly configured SPF, one domain with an SPF record that is invalid due to having too many DNS lookups embedded in it (a

ELECTION SYSTEM MANUFACTURERS: SPF USAGE



SOURCE: VALIMAIL



violating of the 10 lookup limit in the SPF specification), and two domains with no SPF at all. However, SPF alone cannot protect a domain from being impersonated.

This is cause for concern. Election systems manufacturers are a crucial component of the election infrastructure, and if they can be easily impersonated, that provides an avenue for adversaries to disrupt an election, perhaps seriously. For example, imagine an adversary impersonating a manufacturer to send bogus "software update" emails to recipients in various boards of elections in contested states. If just one recipient clicks on the link or installs the fake software update, it could result in compromise of the election board's operational network, or even of election machinery itself.

TAKEAWAYS

It is not difficult to imagine a scenario in which attackers impersonate election officials, state governments, campaigns, or even election systems manufacturers, via spoofed domains, in order to spread disinformation, conduct voter misdirection or vote-suppression campaigns, or even to inject malware into government networks.

For this reason, Valimail urges all organizations involved in elections, from state and local boards of elections to manufacturers to campaigns, to configure their domains with DMARC at enforcement. This step is both feasible, effective, and inexpensive. For instance, the U.S. Department of Homeland Security issued a directive in late 2017 (BOD 18-01), mandating that civilian executive branch agencies use DMARC at enforcement on all of their domains by early 2019. As a result, nearly 80% of the federal government's domains are now protected from impersonation, according to Valimail's research.

The American Bar Association recently called on the U.S. federal government to "empower the National Institute of Standards and Technology (NIST) to establish standards for election software, develop a certification process, and review the private sector role in election systems." Valimail supports this call, and we would add that DMARC enforcement should be a requirement for all domains involved in elections, just as the DHS mandated it for executive branch agencies.

The U.S. Election Assistance Commission offers resources on improving election security, for voters and for election officials, which provides a wealth of useful, actionable information.

Governments and organizations that want to take the first step on their journey to DMARC enforcement can check the status of their domains using Valimail's free, instant domain checker, at valimail.com. This will tell you exactly how your SPF and DMARC records are configured, and what needs to be fixed, if anything.

As a guide for getting started with DMARC, we also provide a free, 44-page Email Authentication Handbook, a detailed, step-by-step guide to implementing email authentication using SPF, DKIM, and DMARC.

DMARC enforcement is a crucial best practice for stopping the largest attack vector into any organization. The low rates of deployment of this open standard among domains involved in elections is a signal that best practices to protect democracy are missing in many key places. It is time to direct funding toward implementing such best practices, with DMARC at the top of the list, across state and local infrastructure.

As we wrote last year, the playbook on how to achieve that is well known, and funding is available. It's past time to get it done.

ABOUT VALIMAIL

Valimail manages DMARC for more domains than any other vendor, and also has the highest rate — and greatest speed — of getting customers from monitoring mode to DMARC enforcement. Our free product, DMARC Monitor, provides an easy way to interpret DMARC reports, helping you understand just which servers and services are sending email "from" your domain.

In addition, Valimail's government products provide the most efficient and effective way to protect government domains from fraudulent use, with the only DMARC cloud solution to achieve FedRAMP authorization for government use. To learn more, visit valimail.com/solutions/government.

We are proud to offer our DMARC solutions for free to national campaigns, government agencies involved in managing or overseeing elections, and election systems manufacturers.

Contact us at democracy@valimail.com for more information.