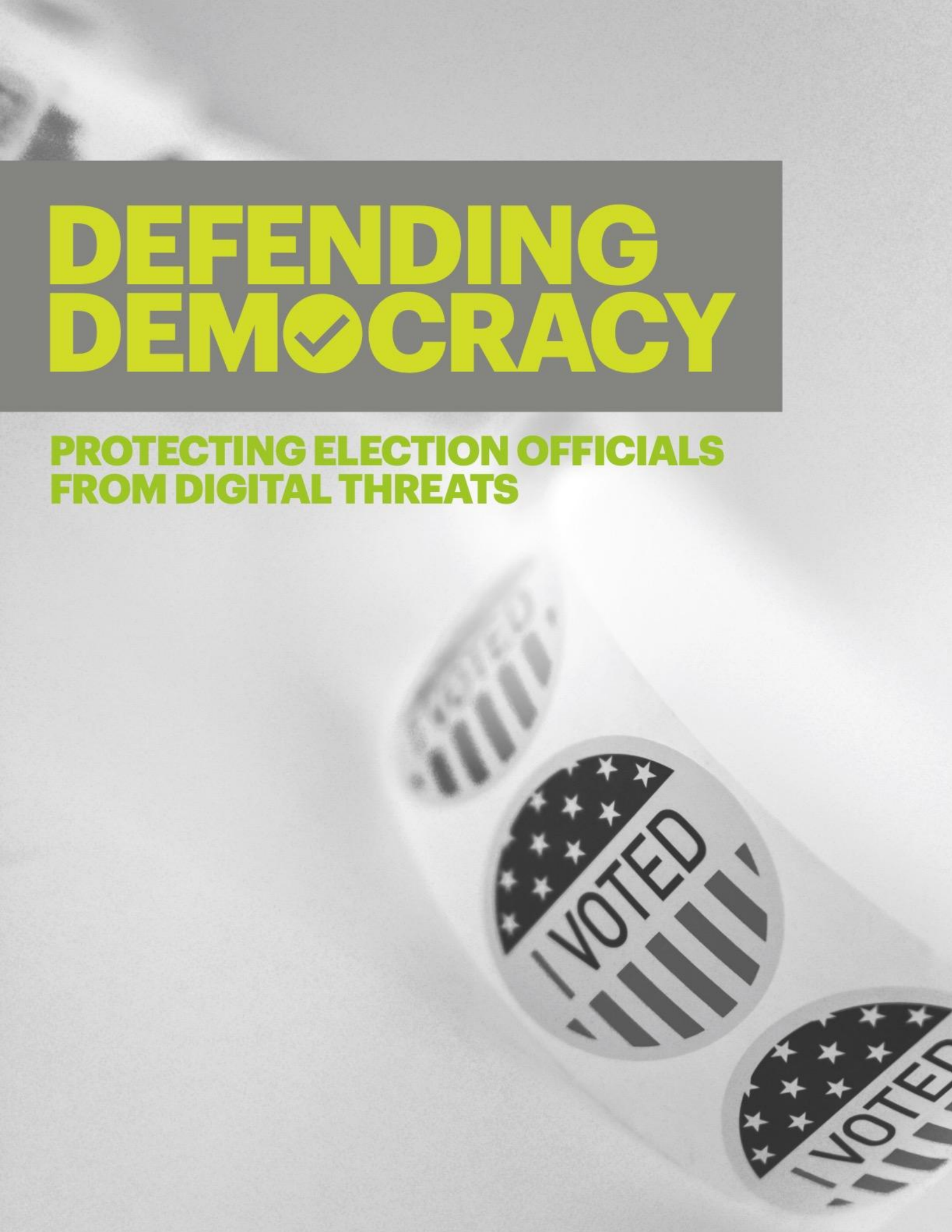
DEFENDING DEMOCRACY

PROTECTING ELECTION OFFICIALS FROM DIGITAL THREATS



1 DEFENDING DEMOCRACY: Protecting Election Officials from Digital Threats

Prepared by Security Positive and The Elections Group. BrightLines is a project of Security Positive.

April 2021

Cover images by Element5 Digital on Unsplash. Design by Gem Barrett.

Contents

INTRODUCTION: A Holistic Approach to your Security

Election officials increasingly find themselves the target of online harassment campaigns with potentially dangerous consequences.

The threats can take several forms, from digital attacks on official infrastructure to an election official's photo and home address shared through extremist networks. Effectively addressing these challenges requires a holistic approach. Even if a threat emerges in cyberspace, the responses must also address possible physical dangers. The digitization of our lives - from social media to public records - means that the boundary between individual and organization safety is increasingly porous. Complex threats warrant nuanced solutions.

We propose a safety planning framework that organizes measures by domain (digital, physical, psychosocial); who should take those measures (individual, organizational); and when to take them (before, during or after an incident). Our full framework, as well as steps to take to shore up your security, is available as an interactive website.

This paper is the first in a series that discusses how to protect election officials in upcoming election cycles. We recommend concrete steps election officials can take in their individual capacities to strengthen their resilience against online harassment that turns physical. While institutional and policy responses are also critical to protecting election workers, they will take longer to actualize.

The second paper in this series focuses on policy proposals to effectively engage law enforcement in addressing threats to the physical safety of elections officials. Additional topics will be determined based on public feedback and interest.

Context for this Paper

The authors would like to preface this discussion with some reassurance. While we list threatening activity from 2020 that forced the issue of personal security for election officials, we are not aware of physical violence targeting an official for their role in the 2020 election. One important purpose of this document is to let election officials know that in the event our country again sees such threats, comprehensive plans exist to provide them with protection.

Help us Test BrightLines

In this whitepaper you'll find a lot of guidance around finding and removing your data from websites in order to prevent attackers from using it against you. We won't lie: the process can be time-consuming and overwhelming. Security Positive is currently developing a service called BrightLines, which is built to take care of the problem for you by finding and removing your personal data from the internet, on your behalf. We'd like to offer you the opportunity to have a free test of the service to help us improve it prior to launch. If you're interested in protecting yourself from digital threats for free, you can sign up at www.brightlin.es.

ONLINE THREATS: WHAT ARE THE DANGERS?

The combination of political unrest and extremists' increasing digital capabilities has resulted in a previously-unthinkable scenario: civil servants, especially those working on elections, can suddenly become highly-politicized figures.

In 2020, online mobs tracked down information about election workers and their families, and shared what they found: home addresses, personal phone numbers, email addresses, and social media accounts. By publishing this data, or *doxxing* their targets, they encouraged online and offline intimidation and threats.

Election officials received angry and threatening calls, as did colleagues, spouses or partners, even extended family. Threats were tailored to the identity of officials: female-presenting officials or loved ones receiving sexualized threats; non-white officials receiving racialized threats. The specter of physical violence was raised, and in some cases culminated with partisans, incited by the online frenzy, physically confronting election workers.

The impact of threats and intimidation on our nation's election workers should not be underestimated. Some felt forced to resign. Key staff left, taking with them crucial institutional knowledge. Others simply feared completing their work at an already difficult time, and experienced emotional trauma.

From lead election officials to temporary workers, and from elected positions to contract employees, no one was immune; Secretaries of state and local officials were harassed and bullied; their families and staff were threatened with violence. Contractors for a voting tech company were threatened with a noose, and a ballot clerk was forced into hiding.

Personal threats against election officials intimidate them in their public capacity, making them fearful of doing their jobs. An attack on one damages the integrity of the system. There are clear impacts, such as the time and resources spent on security, and difficulty attracting or retaining staff.

But it's worth underlining subtler implications. Imagine an official noticing an easily remedied, honest mistake, but ignoring it out of fear that admitting error could put them in danger, regardless of who the error favored. Or failing to speak on behalf of a colleague wrongly accused because it could draw menacing attention their way. When online mobs attack

election integrity, the scattershot destruction may not be limited to their enemies. An attack on one may affect the ability of others to do their job, and endanger our democracy overall.

TYPES OF THREATS AND ATTACKS OF 2020

Almost every 2020 incident began with an online mob working itself into a frenzy online, and escalated from there to other activities. Understanding the levels of threat represented by these different activities is key. We address the threats 2020 surfaced in the latter half of this document and in our online tool, found here. Below is a common progression of threat activity, though threats may emerge at any point.

MISINFORMATION BREEDS ONLINE DISCONTENT

Online efforts to examine unsatisfactory election results may be an exercise in healthy skepticism, hunting for errors without jumping to conclusions about what happened or why. This hunt can be alarming nonetheless, because **too many are driven by the assumption that their candidate has been or will be cheated, and the only question is finding out how**. Online supporters of the perceived-wronged candidate pore over videos and statistics, searching for anomalies that are easily explained by someone with an understanding of election procedures. In partisan online forums, anomalies are greeted with naive outrage rather than recognition that context may explain them, and misinformation is quickly passed along.

Senior election officials recognize that they are public figures, with a realistic expectation of some critical public and media attention. But staff and poll workers are not public figures. **Learning that their faces or names are circulating in public forums alone may frighten them**. And before the mob settles on a different scapegoat, the scrutiny is unsettling.

What: Online mob video scrutiny
Who: Poll workers and junior election staff
Where: Multiple jurisdictions
Details: Many offices provided video of ballot counting as a token of transparency. And observers used phones to take footage. In some instances, video was uploaded to forums where an online mob tore into it, zeroing in on actions of frontline staff, and inventing personas and motives for them.

What: Amateur statisticians
Who: Election officials and vendors
Where: Swing state counties
What: Online commenters called out results they found shocking in specific suburban counties, though results in suburban counties nationwide shifted similarly. They suspected military ballots too, though the batches in question came from citizens overseas or soldiers from minority communities.

As soon as discussion or footage of the office shows up in online forums - even before the angry messages arrive - steps should be taken to document the threats, protect staff, and thwart potential escalation.

AMPLIFIERS RECRUIT AN ONLINE MOB

Online mobs could form against an election official in a couple of ways. They can develop organically from the complaints or charges originating locally. Online sleuths in 2020 pointed to thousands of details, mostly innocuous, none outcome-changing, that they found suspicious. All helped create the toxic atmosphere that went beyond distrust to create certainty for many that the election was rigged. Only a few of these complaints became the focus of online mobs.

In other cases, targeted individuals find themselves identified by prominent figures as an enemy, either directly or by association. The reasons for the targeting can vary, from misinformation, misunderstandings of the election process, or suspicion surrounding COVID-related process changes. While even the most disillusioned online sleuths' complaints were unlikely to go viral in 2020, if a prominent social media figure amplifies a complaint, the online group can quickly grow from ineffectual to menacing. Foreign adversaries, domestic troublemakers, or politicians all may fan the flames of discord.

THREATS TARGET REAL PEOPLE

Fielding misguided complaints from angry callers can be upsetting and intimidating. **But when individuals are identified and targeted, the implication of violence becomes explicit**, whether verbally or by violent imagery. Messages are often racialized or tailored to a victim's identity, with symbols like nooses, mentions of rape, or criminal trial and execution.

Whether the targeted individual is a public figure or less visible staff member, their identification by well-known instigators can spread easily and quickly across social networks.

Once the target's name has been identified and spread, their personal information is then sought out so they can be subsequently attacked in a **'doxx'.** This personal information commonly includes home address, phone numbers and email or social media accounts.

DEFINITION

"To dox (or doxx) someone is to publicly identify or publish private information about that person —especially as a way of punishing the person or getting revenge." - Merriam Webster dictionary

What: Naming and doxxing
Who: Mail ballot clerks
Where: Swing state counties
What: In multiple forums, online mobs published the names of staff in videos, doxxed them, and in some cases even tracked down names, addresses and contact info of family members of the staff involved. Angry calls and messages were directed to public and private points of contact.

What: A death threat list
Who: Senior election officials and governors
Where: In multiple jurisdictions
Details: The website, "Enemies of the People," targeted officials in swing states and others who publicly said the election was fair. The site, attributed to the Iranian Government by the US intelligence community, called for their assasination, posting their faces in crosshairs along with home addresses.

HARASSMENT EXTENDS TO FAMILY & FRIENDS

Attacks commonly extend to a target's network of family and friends to add pressure, and increase fear and intimidation. Attackers use details, such as mentioning a sibling's name in messages or harassing a child's social media accounts. If the information is available, they can also extend the harassment to coworkers or a partner's employer.

Who: Canvassing board members
Where: Swing state
What: After refusing to certify the election results, members of the Board of Canvassers saw their names, personal details and links to their social media accounts spread across Twitter.

Who: City commissioner
Where: City in a swing state
What: The commissioner and his staff were threatened when he defended the local vote count, triggering a doxx of phone numbers. They received multiple death threats and attacks, some of which were anti-Semitic.

SOCIAL MEDIA DELIVERS ATTACKS

Social media is often the vehicle for gathering information about a target and coordinating and delivering an attack on them. Personal social media profiles reveal a lot about a person and the people who are important to them. Harassment on social media can occur in replies to a user's own posts, as attackers heap abuse in a dogpiling attack.

Not having a profile doesn't exempt a target from abuse. The platform can still be used to escalate harassment because of the widespread nature of social media platforms. Facebook and Twitter, for example, often play host to doxxing attacks because attackers can spread a target's personal information faster than it can be taken down. Alternate apps such as Parler,

and message boards like Reddit, 4Chan and 8Chan are also widely used to host online harassment and share doxxed information. Most popular platforms have policies on doxxing, which are enforced to varying degrees. While reporting the posts and the users sharing them may get platforms to remove private information, this can be hard to do in the middle of a crisis.

For practical steps you can take to deal with doxxing, see **4 ways to protect yourself when under attack**.

What: Doxxing via social media
Who: Secretary of state
Where: A swing state
What: A secretary of state was doxxed via Parler, where users posted her phone number and home address and encouraged people to show up at her house.

What: Lynching threat via social media
Who: A state representative
Where: A swing state
What: A legislator criticized the invitation of Rudolph Giuliani to an election hearing. She was doxxed and received a barrage of ugly, racist emails, one of which mentioned lynching her.

ONLINE ATTACKS MOVE TO OFFLINE THREATS

What began online in 2020 threatened to culminate in real world attacks. Harassment online is harrowing enough, but repeatedly online mobs crossed the digital divide to intimidate election workers with a variety of real world, physical threats. The trauma of receiving ugly, intimidating messages should not be underestimated, even if no violence occurs.

Who: Young voting-system contractor
Where: Swing state
What: A video shared online falsely claimed to show a contractor engaged in “ballot harvesting,” when in fact they were saving a data report to a thumb drive before filtering the data on a laptop. One man seen in the video was identified by name and was subsequently doxxed on 4chan and Twitter. His family was also harassed and a noose was found at his door.

Who: County IT staff
Where: Swing state county
What: Workers moving non-election equipment were followed for 10 miles by someone live-streaming the incident to Twitter. Unable to evade their pursuer, they called 911, remaining in their car until police arrived, to avoid provoking an incident.

Online threats function as a kind of mental rehearsal, and should be seen as a legitimate precursor to someone actually taking violent action. Any mention of violence should trigger security measures. See our section **Tackling Online Violence Before it Moves Offline** for steps to document, report, and safeguard against these threats.

DEFINITION

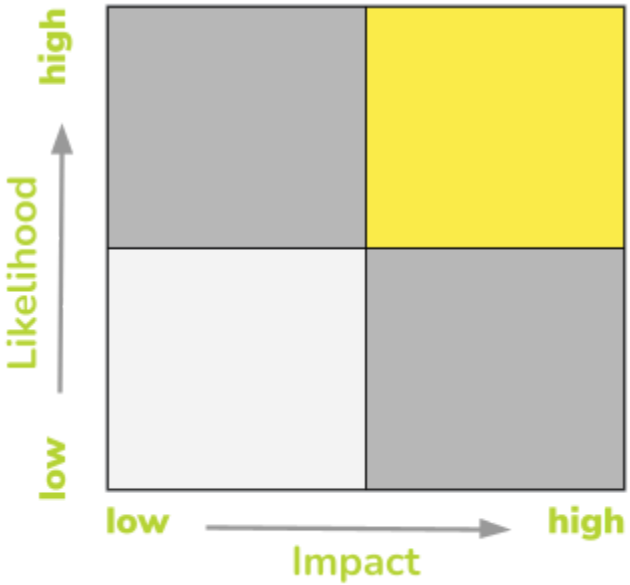
"[Dogpiling]: a large group of abusers collectively attacks a target through a barrage of threats, slurs, insults, and other abusive tactics." - Online Harassment Field Manual

LIKELIHOOD AND IMPACT OF THREATS

In security planning, threats are prioritized along a matrix of likelihood and impact. Threats that land in the high likelihood / high impact corner are those that deserve the most attention the soonest.

LIKELIHOOD AND LIKELY?

An attack is likely if: 1) it has already targeted a person; 2) it has targeted others like that person; 3) the attacker is the same or similar, or follows a similar pattern in their attack. For example, commonalities in the way that election officials are harassed, and the methods by which those attacks escalate, demonstrate a likelihood of attacks using personally identifying information (PII) found online.



PII of a target is a crucial part of the attackers' arsenal. Attackers can piece together a surprisingly complete picture from social media, online public records, data broker sites and hacked accounts.

Doxxing is the link between PII and the escalation to offline harassment and threats. For marginalized groups, doxxing can be particularly dangerous as it can lead to attacks based on race, gender, and other identifiers that can be a target for prejudice. Stalking and swatting are two threats which can arise from doxxing and are dangerous for anyone, but pose additional risks to people with marginalized identities.

There are steps to take to minimize this vulnerability, namely, removing PII from the internet. The more PII removed from the internet, the less there is for an attacker to use when building a picture of an official's assets and network.

OVERT AND UNANTICIPATED IMPACTS

Attacks against election officials can have a range of negative impacts, the severity of which is determined by a person's economic and social status, physical and mental health, and aspects of their identity, such as gender, race, age, and ability. Officials may be forced from their job due to political pressures, or have their financial stability affected by identity theft or the consequences of bringing, or defending against, legal action resulting from the attacks. To stop phone harassment or intimidation, officials may need to shoulder the costs of changing phone numbers or even moving.

Attacks take their toll on mental health too. Receiving threats against yourself or your loved ones creates stress and can leave you feeling overwhelmed and isolated, which, over time, can lead to burnout, depression, anxiety and Post-Traumatic Stress Disorder (PTSD). Physical health conditions can also re-emerge as a result of attacks, and reputational damage can exacerbate health damage. In some cases these impacts can lead to resignation. **Over the course of 5 months in 2020, more than 20 local election administrators across 6 states retired or resigned due to burnout, stress or health concerns**.

Attacks can erode trust among colleagues, within professional networks, and across family lines. An official may fear that admitting an error could put them in danger, or that associating with another official who erred could draw negative attention. Attacks that mar officials' reputations can strain their professional relationships. If attacks spread to friends and family, they can create issues with those relationships, too.

TACKLING ONLINE VIOLENCE BEFORE IT MOVES OFFLINE

The following checklists are actions to take to shore up security against these particular threats before, during, and after an attack. Because it can be harder to find support as the attack escalates, proactively planning and taking preventative measures can decrease the likelihood of an escalation as well as reduce the impact of an attack.

BEFORE: 4 STEPS TO SECURE YOUR ONLINE PRESENCE

1

Search for personal identifying information online. This can include email addresses, photos of you, and phone numbers. For more information on finding personally identifying information (PII) see our 'Manage your Online PII' guide.

✔ Search for your PII with Google or a privacy-conscious search engine such as DuckDuckGo, trying out different combinations of your name, address, phone numbers, etc. See our online guide for suggested searches.

✔ Look for images of yourself online to see what they reveal about your relationships, your usual locations like gym or restaurants, or for links to profiles you may have forgotten about. You can use Google Image Search or reverse image search tools such as PimEyes and TinEye.

✔ Websites such as HaveIBeenPwned are useful for discovering whether your email addresses have been exposed in a data breach, and we recommend signing up to be notified if they are exposed in future breaches.

✔ If you have ever listed a business online you may find it linked to your home address on maps services. Be sure to search business names with your addresses. Maps can also provide information about your favorite, frequently visited locations thanks to check-ins and reviews you've posted.

2

Scrub old information and close old accounts. The process of identifying and removing PII can be time-consuming. Use services like JustDeleteMe.xyz, Delete Me, Kanary, and Reputation Defender to manage parts of this process.

Security Positive, one of the organizations co-authoring this white paper, offers a new PII management service called BrightLines. More information about the service and how you can sign up as a tester can be found here.

To help prioritize PII removal, consider:

✔ How easy is it to access PII on each site; would someone have to pay to access it, or open an account with that platform?

✔ Whether the PII or other online data could be presented in a way that damages your reputation, or causes other harms to you and your loved ones.

✔ How much time you spend on each platform. Different platforms have different processes for removing information and deleting accounts, and some make it harder than others.

3

Secure your accounts with complex passwords and two-factor authentication. Any old accounts that can't be closed need to be protected, too, so attackers cannot access anything potentially embarrassing to share publicly. For more details and resources see our 'Shore Up your Accounts' guide.

✔ Identify the most valuable accounts and note who has access to them, and which security measures have already been implemented on them. We suggest prioritizing email and cloud accounts, bank accounts, chat apps, and websites.

✔ **Two-factor authentication (2FA)** is a method in which a user is granted access to an account only after presenting two pieces of evidence of ownership. The method requires a combination of something you know and something you have, such as a bank card and a PIN at an ATM, or a password and a numeric code linked to your phone. It can also require something you are, like a fingerprint, voice recognition or location.

✔ **Passwords:** To be effective, passwords must be: complex, unique and secret. Visit HowSecureIsMyPassword to test password strength, and use HaveIBeenPwned's Password Checker to see if it's been exposed before.

✔ To make a long, complex password that's also easy to remember, use spaces, words from other languages, or mantras or phrases that are NOT linked to social media profiles or online data, such as an address. We recommend a three word format, i.e., "bicycles bourbon fireworks;" it's easy to remember, and at 26 characters will take over 8 septillion years to crack. Special characters are optional.

✔ Set up 2FA with all accounts that offer it. You will need to install an authenticator app like Authy, Duo Mobile or Google Authenticator on a mobile phone or use the less secure (but better than nothing) SMS messages method.

✔ Keep track of unique passwords with a password manager. It can auto-generate long, unique passwords, which are then stored in encrypted format to protect them. It can also work across devices. We recommend Dashlane, BitWarden or LastPass.

4

Create alternative public-facing contact information. Adding an extra layer between your communications and the rest of the world can help to protect actual contact information from would-be doxxers. For more information about alternative contact points see our 'Manage your Online PII' guide.

✔ Set up a virtual phone number to share an alternate phone number with online services, doctors offices, and others who are relatively unknown. Calls may then be forwarded to a phone or silently blocked, relying on voicemail transcription to screen calls. Voicemail can also assist with documenting the harassment and threats. Most importantly, it's easier to change a virtual number than a personal phone number, if needed. We recommend a virtual number through Google Voice, eVoice or TelNum.

✔ Create a public-facing email address that forwards to an actual, main email account. The public account is used anywhere on the web: to log in to social media and e-commerce accounts, and sign up for newsletters. It is not an inbox, so set it up to forward email and not keep it in the inbox. This limits the exposure of your actual email account, making it harder to both flood with messages and to hack.

DURING: 4 WAYS TO PROTECT YOURSELF WHEN UNDER ATTACK

1

Mute, block and report the harassers. These measures can limit your exposure to attackers on personal social media profiles and accounts. Yet, the balance obviously must be struck for a public official to maintain transparency. See our guide for strategies for dealing with trolls.

✔ Follow the guides each social media platform produces for using their **abuse reporting tool**. We recommend starting with Twitter, Facebook and YouTube.

✔ **Block an account** so neither you nor the attacker can see or contact each other on that platform. Be aware: harassers will know they've been blocked and may escalate the harassment through new accounts.

✔ Ask for help from friends, colleagues, or IT departments if you want to monitor blocked accounts or topics, as the abusive posts may proliferate. Reported abuses may also be dealt with faster if the platform receives multiple reports.

✔ Tools like Block Together and Block Party can help to share the burden of dealing with harassment on Twitter. They both involve a network of trusted people to help manage the blocking and filter out unwanted interactions.

✔ **Mute accounts, comments, messages and keywords,** depending on the platform. This hides people, conversation or topics from your view. Muted accounts and messages can continue but are no longer visible to you by default.

✔ Many platforms allow for locking an account to restrict interactions to just followers, and new followers each have to be approved. This leaves trolls or attackers among existing followers, but setting an account to private can still help to stem the flow of harassment on that platform.

✔ Check settings on the social media platforms that host the harassment, as there may be other ways to restrict interactions. For instance, disallow location and photo tags.

2

Document the abuse. It can be useful later on to have documented the harassing social media messages, texts, emails and calls, especially if you decide to pursue legal action. For more on documentation, see Pen America's Online Harassment Field Manual.

✔ Use your device's default method for capturing images directly from a screen, or download a separate app. Screenshot the abuse received on social media, and store it in an easy-to-access folder. Get hyperlinks where possible.

✔ Move any emailed harassment out of the inbox and into a separate folder. If there's a pattern to the content, set up a filter to move emails automatically. Retain emails as they contain important meta data header that identifies the sender.

✔ In the midst of a crisis it can be hard to see the point in this time-consuming task, but gathering a record of what happened can be critical if the situation escalates. If it becomes too much, ask a trusted confidante for help.

✔ Log threatening calls and voicemail messages in an incident log, including the date, time and number of each telephone incident, even if calls are coming from out of state.

✔ Screenshot abusive texts.

3

Warn your network. If the attack is escalating, and concern grows for your friends and family, let them know about the threat you're currently facing, and that they might also face, so they can protect themselves and be prepared.

✔ Determine which contacts are most likely to be impacted by an attack against you, and warn them first. Offer security steps for them to take.

✔ Warn IT and office security teams, even if the abuse is on personal accounts at the moment. If work-related accounts are under attack, the IT team should be able to help retain control.

✔ Alert those who are close but unlikely to be attacked that they may hear some nasty and confusing things, and why. Getting ahead of the attempts to damage a reputation can help to lower the attacker's credibility.

AFTER: RECOVERY AND LEARNING

When the harassment lets up, take time to assess what happened and how it happened. This is important for three reasons:

✔ Contemporaneous documentation helps backup a version of events if you intend to take legal action or seek prosecution of attackers. It may also clarify your understanding of events.

✔ If additional incidents occur, notes may help recognize a pattern and act to break the cycle. For instance, if a specific attacker sends harassment after your gives interviews, steps can be taken to adjust your online presence accordingly prior to future interviews.

✔ The debrief will identify areas in which to tighten security, resurface ideas had during the incident, consider what could have been done better, and also which aspects of managing the situation might have been delegated to others. For example, a tech-savvy person may be better for managing your Twitter mentions. Or more PII online may live online than previously realized, and a professional service may be needed to help with it.

Just getting through a very traumatizing experience is enough. Documenting the threats or asking for help is a bonus. It's common to suffer with anxiety and even panic attacks after facing online abuse. It's important to take care of yourself after an attack, both emotionally and physically, and to reach out to those impacted by the attack on you to offer support.

CONCLUSION

The 2020 election saw dedicated public servants, working under tremendous pressure and scrutiny, run the most secure election in modern history while being subjected to targeted attacks online and real, personal threats offline. We saw first-hand the stress caused by the tsunami of concerned and cynical citizens who contacted election officials. And the anxiety of the increasing potential for personal threats and doxxing, as you kept hearing about the threats to your colleagues.

To that end, we wanted to provide some guidance around how to protect yourself personally, starting with how to find and remove your online data to prevent attackers from using it against you. Although it's preferable for attacks to be directed at your work email and social media account, where you often have the support of internal IT and legal departments, we know that it is you that's the target, not your job. Attackers happily invade personal email or social media accounts where you don't have that same support, and the intrusion into your personal life can be that much more terrifying and intimidating.

All of the checklists in this paper are offered in an online tool that helps you plan, both as an individual and within your organization, for digital and physical threats before, during and after a crisis. We also offer more detailed steps to identify and scrub your PII, key to decreasing the likelihood that an online attack moves to your offline life. If you're interested in testing BrightLines with your online profile, see our website at www.brightlin.es.

Our online tool also provides guidance for securing your devices and your work-from-home setup, and strategies for incident response planning, managing trolls, and working with law enforcement. Keep an eye out for a forthcoming piece from The Elections Group on building cooperation with law enforcement to help you identify the agencies and protective services from which to seek help, and the strategies to ensure information is shared quickly.

BRIGHTLINES www.brightlin.es
SECURITY POSITIVE www.securitypositive.com
THE ELECTIONS GROUP www.electionsgroup.com