SPECIAL REPORT

CREATING A CYBER VOLUNTEER FORCE: STRATEGY AND OPTIONS

March 2023

McDermott
Will & Emery

McDermott
Will & Emery

TABLE OF CONTENTS

LEARN MORE

For more information, please contact:

MARK E. SCHREIBER
SENIOR COUNSEL | BOSTON
mschreiber@mwe.com
Tel +1 617 535 3982

BRIAN LONG
ASSOCIATE | DALLAS
brlong@mwe.com
Tel +1 214 295 8085

AUTHORS

MARK E. SCHREIBER
SENIOR COUNSEL | BOSTON

SCOTT FERBER
PARTNER | WASHINGTON, DC

BRIAN LONG
ASSOCIATE | DALLAS

PETER SCHEYER
LAW CLERK | WASHINGTON, DC

ROBERT DUFFY
COUNSEL | WASHINGTON, DC

MARINE MARGARYAN
ASSOCIATE | WASHINGTON, DC

CATHY LEE
ASSOCIATE | WASHINGTON, DC

AMY C. PIMENTEL
PARTNER | BOSTON

This is a pro bono project of McDermott Will & Emery LLP.
Each of the authors is a member of the Firm’s Global Privacy & Cybersecurity Practice Group.

We are also indebted to the government officials and numerous individuals at nonprofit entities and universities who provided invaluable insight for this project.

The information contained in this study is for informational purposes only. This study and documents do not create an attorney-client relationship between McDermott Will & Emery LLP and you, and are not legal advice. Legal advice must be tailored to the specific circumstances of each case, and the contents of this study are not a substitute for legal counsel. Do not take any action in reliance on the contents of this study without seeking the advice of counsel.

I. EXECUTIVE SUMMARY AND RECOMMENDATIONS

Our country's critical infrastructure and essential services are highly vulnerable to disruptions from cyber attacks. Many companies and organizations are underprepared for a large-scale cyber attack. This is especially true of small or rural critical infrastructure entities, which lack robust IT or experienced security personnel. Not only has the cost of a data breach reportedly "reached an all-time high" of $4.35 million, but the average cost of a data breach for critical infrastructure organizations is now $4.82 million—$1 million more than the average cost for other industries.[1] Many of these small or rural critical infrastructure entities lack cyber resilience and are unable to run mature information security programs or mount an effective incident response.[2]

Given the ever-growing need for cybersecurity services in all sectors and the inability of the marketplace to keep up with demand, a number of entities have begun organizing cyber volunteer efforts to provide needed cybersecurity assistance to resource-deprived recipients. Expanding the ranks of cybersecurity volunteering efforts would align with the recently updated National Cybersecurity Strategy.[3] States, national guards, emergency response organizations, for-profit and not-for-profit organizations, universities and legislators have built programs to support volunteers who are tasked with improving cyber preparedness. There has been discussion also of a potential federal model to integrate volunteers that has not yet been realized.

Each model has notable strengths and challenges. Each could be expanded over time but with various ramp-up or time horizons, complexities or limitations. Even more cyber volunteers are needed, but the process of effectively identifying, recruiting, vetting and deploying volunteers in the United States poses a number of unanswered questions and issues. To date, there have been few, if any,

[1] IBM, *Cost of a Data Breach*, at 5 (2022) (https://www.ibm.com/downloads/cas/3R8N1DZJ) [hereinafter "IBM Report"].

[2] As the U.S. Cyberspace Solarium Commission observed in its March 2020 report, "resilience" is a "foundational element of layered cyber deterrence, ensuring that critical functions and the full extent of U.S. power remain available in peacetime and are preserved in crisis." U.S. Cyberspace Solarium Commission March 2020 Report, at 55 (https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report/) (last accessed Feb. 6, 2023).

[3] National Cybersecurity Strategy, Strategic Objective 4.6, 27, (Mar. 2023) (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf) ("To recruit and train the next generation of cybersecurity professionals to secure our digital ecosystem will require Federal leadership and enduring partnership between public and private sectors.") [hereinafter "National Cybersecurity Strategy"].

comprehensive studies of cyber volunteering models, best practices and relevant legal issues. Potential solutions remain untapped and lightly explored, with a number of these organizations unaware of others or siloed to a degree.

The following steps (both short-run and long-term) are critical to achieving a more mature integration of the diffuse cyber volunteer efforts in the United States:

- **Volunteer Resource Platform**: There needs to be a dedicated effort for coordination of the various cyber volunteer programs currently in existence. This should include a knowledge management function—supported by the US Department of Homeland Security (DHS), its Cybersecurity & Infrastructure Security Agency (CISA) and others—that catalogs which organizations are providing volunteer services and what volunteer services are offered. It should also help translate successful practices from the different models and facilitate the sharing of best practices among organizations. Implementation could be provided through an ongoing agenda item for the CISA Cybersecurity Advisory Committee and coordination with CISA's Joint Cyber Defense Collaborative (JCDC), to include, at minimum, creation of the following:
    - A **national website** that lists the various cyber volunteer programs in their respective categories with updated service and contact information
    - A **national, annual conference** to champion and organize coordination between the various cyber volunteer programs, which should be interdisciplinary among the various models of cyber volunteer organizations to promote the development of best practice capabilities, forms and playbooks, and recent lessons learned from the field[4]
    - A **common set of metrics** (*e.g.*, numbers of requests for assistance, completed cyber assessments/missions, completed incident responses, active volunteers and length of service, attrition rates, and types of beneficiaries and industry sectors) to better track success across cyber volunteer programs and to serve as a

[4] While we have identified a number of best practices and created certain model forms, as in Appendix 3, clearly there is more to be done. Additionally, we note that there are efforts underway towards conferences such as the Cyber Civil Defense Summit scheduled for June 2023 by the UC Berkeley Center for Long-Term Cybersecurity (https://cltc.berkeley.edu/).

measure for authorities and interested donors to determine effective ways to contribute[5]

- **Self-Assessments**: Each cyber volunteer organization should periodically perform a careful analysis of its distinct capabilities regarding cyber assessments and incident response work by volunteers because of the different skillsets and types of services required for each of these categories. Many organizations, by virtue of their model and structure, may be more suited to one service rather than the other.

- **Model Legal Agreements**: Model legal agreements among the volunteering parties should be created, distributed and periodically updated for cyber volunteers and cyber volunteering organizations as a starting point for the complex legal issues that need to be addressed, e.g., responsibilities, scoping, confidentiality and indemnification. We prepared a model cyber volunteer agreement. See Appendix 3.

- **Analysis of Non-US Organizations**: A review of relevant nonprofit organizations outside of the United States, especially those in Switzerland, the European Union and the United Kingdom that have engaged cyber volunteers in a developed fashion, should be performed to better understand advances and other best practices applicable to the United States.

- **Grassroots Efforts**: Cyber volunteer organizations should consider creating local groups for individuals to connect with other volunteers in their community and have a platform for exchanging knowledge and expertise.[6]

- **Nonprofit-Specific Considerations**: There should be a centralized nonprofit cyber entity that identifies donors, beneficiaries and individuals coupled with a matchmaking platform or service. This entity could organize cyber volunteer services directly, serve as a clearinghouse to connect beneficiaries with other organizations or both. This nonprofit entity should similarly designate a website containing an overview of all nonprofit organizations offering cybersecurity services or link to the CISA-supported website.

[5] See discussion on Aspen Digital and philanthropist Craig Newmark's contribution, *infra*, note 58.

[6] See IAPP KnowledgeNet Chapters as an example of a professional network with local privacy and cyber groups: (https://iapp.org/connect/communities/chapters/) (last visited, Jan. 20, 2023).

- **NET Guard Follow-up**: It would be valuable to have access to an after-action report (if one exists) or any further anecdotal evidence following the 2008 rollout of FEMA's National Emergency Technology Guard (NET Guard). Knowing the outcomes from a program that had statutory support, government funding and a four-city rollout could help others understand how to better allocate funding, what further legislation is necessary and what issues other cyber volunteering efforts may face.

The various cyber volunteer models (including nonprofit, corporate, state/local governments, academic institutions and federal government) have their own strengths in terms of their cyber response roles. For example:

- The nonprofit option seems to be the most suitable for cyber assessments and modest incident response, at least in the near term.
- State-based volunteer models have greater efficacy with incident response work that may be needed for larger scale or local cyber events.

Each of these models has successful practices that can be translated or adopted by others, and a platform should be developed whereby volunteer organizations can avail themselves of the lessons learned. The following elements are critical to the success of certain cyber volunteering models, which may be adapted as appropriate:

- Creation of an effective infrastructure, including software to automate the posting of potential pro bono work for recipients that is used as a matchmaking service with volunteers

- Monitoring of the performance of the volunteers with a feedback loop for the recipients

- Reliance on corporations that volunteer their resources to vet the individual employee volunteers for appropriate skills, thereby avoiding repeat, costly background checks, forms and hiring evaluation processes

- Development of model agreements between corporate partners, the individual volunteers and the beneficiaries/recipients of the free services

Additionally, we have discovered at least one instance where a nonprofit organization, Geneva-based CyberPeace Builders,[7] has built a model that

[7] CyberPeace Builders, which is a program of the Cyber Peace Institute, currently focuses on free cyber services for NGOs globaly. *See* CyberPeace Builders (https://cyberpeaceinstitute.org/cyberpeacebuilders/).

incorporates most of the above features and potentially could be replicated in the United States. CyberPeace Builders approaches corporate volunteers to allow their skilled cyber employees to donate their time, and a number of US companies have contributed, such as Microsoft, Mastercard, Rapid7, Okta and LinkedIn. Due in part to an effective implementation of matchmaking software to automate the process, the model is scalable, to a point, for cyber assessment services, and CyberPeace Builders reportedly has upwards of 110 beneficiaries with approximately 300 volunteers actively serving them on missions.

Nonprofits are limited in their incident response capabilities, and we must rely on the expansion of the state model for effective incident response to major or industry-wide attacks, unless the federal government decides to further engage in cyber volunteer efforts. While there is no national policy or task force on cyber volunteering,[8] CISA could provide a strong and enduring voice in achieving these cyber resilience objectives with volunteer organizations.

II. THE NEED FOR CYBER VOLUNTEERS

INTRODUCTION

In this study, we review existing efforts to organize cybersecurity volunteering efforts and propose solutions to expand the effectiveness and reach of the collective cyber volunteer force.

The need for these services is vital. The average cost of a data breach in critical infrastructure is $4.82 million per data breach, 22.9% higher than in other industries.[9] An estimated 28% of data breaches occur in small businesses, and 55% of ransomware attacks hit businesses with fewer than 100 employees.[10] Critical infrastructure is particularly vulnerable, as smaller entities in this sector often lack the resources to deploy existing cybersecurity tools. For example, 79% of critical

[8] The National Governors Association recommended that there should be a national task force "composed of public, private, and academic stakeholders to inform policy considerations that account for key players' interests, concerns, and independent assessments . . . [and] will include . . . the likely recipients of the volunteer response services and the industry and academic partners from which volunteers are likely to be sourced." The National Governors Association, *Re-Envisioning State Cyber Response Capabilities: The Role of Volunteers in* Strengthening *Our Systems*, at 17 (2022) (https://www.nga.org/publications/re-envisioning-state-cyber-response-capabilities-the-role-of-volunteers-in-strengthening-our-systems/) [hereinafter "NGA Report"].

[9] IBM Report at 4, 5.

[10] Jeff Bell, *Small Business Cybersecurity 101: Simple Tips to Protect Your Data* (2021) (https://www.forbes.com/sites/forbestechcouncil/2021/06/14/small-business-cybersecurity-101-simple-tips-to-protect-your-data/?sh=40e98b194679).

infrastructure providers do not use a zero-trust framework.[11] Additionally, there is no clear correlation in the NetDiligence study between the size of the organization and the magnitude of the cyber-related loss, meaning even small entities can also suffer significant damages or effects.[12]

The latest IBM study shows that employing these tools dramatically reduces the cost of a data breach and the time needed to respond. Software tools such as artificial intelligence (AI) and extended detection and response (XDR) "significantly reduce average data breach costs and breach lifecycles."[13] As well, "having an IR [incident response] team and regularly tested IR plan led to significant cost savings."[14] Volunteers, particularly those trained in such tools, can have similar impacts. Organizations that use such tools see an average savings of $3.05 million per breach compared to those who do not.[15] The impact of automation should not be understated, and this is an area where experienced cyber professionals assisting smaller organizations with deployment could be particularly effective in preventing or remediating cyber incidents. Entities using cloud services are also not immune to these considerations, as 45% of breaches occur in the cloud.[16]

The demand for such human resources has, however, outstripped the supply. In the United States there are reportedly more than 750,000 open positions in the cybersecurity field, which translates roughly into a 40% deficit of such open positions.[17] Globally, there may be close to 2 million cybersecurity job vacancies.[18] The shortage of trained personnel and companies providing cybersecurity services makes the situation even more dire. "The consistent shortage of cybersecurity

[11] IBM Report at 4.

[12] NetDiligence Cyber Claims Study, 2022 Report, 4, https://netdiligence.com/cyber-claims-study-2022-report/.

[13] *Id.* at 48.

[14] *Id.* at 7.

[15] *Id.* at 5.

[16] *Id.* at 39.

[17] Cyberseek.org (https://www.cyberseek.org/heatmap.html) (last visited, Jan. 20, 2023). "Despite an increase of 700,000 cyber personnel in the global labor market over the past year, the demand for this talent pool continues to outpace supply." NGA Report at 7; National Cybersecurity Strategy, 31 ("Today, there are hundreds of thousands of unfilled vacancies in cybersecurity positions nationwide, and this gap is growing").

[18] The Secretaries of Commerce and Homeland Security, *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce*, at 23 (2017) (https://www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf).

personnel represents a high risk to national security,"[19] according to a recent Senate report accompanying a Civilian Cybersecurity Reserve proposal.

CISA, a federal agency within DHS, is responsible for protecting the nation's critical infrastructure and supporting the cybersecurity of federal civilian agencies. CISA has, to its credit, developed an extraordinary number of detailed programs and initiatives to help with cybersecurity alerts, mitigation steps and protocols. However, keeping up with CISA's advances requires additional resources and tools, particularly for small organizations, which struggle to find, retain and competitively compensate cybersecurity professionals.

CISA has done a remarkable job in closing the cybersecurity research, knowledge and awareness gap, but the implementation gap still defines the industry in many ways. Determining how to implement CISA's advice, alerts, frequent updates and mitigation steps is a constant challenge for even the most sophisticated organizations. Many organizations may struggle to apply and implement cybersecurity principles to prevent and mitigate attacks, including CISA's advice. IT professionals in most organizations are already overworked and, in some instances, may lack expertise in cybersecurity assessments and necessary measures.

SCOPE AND PURPOSE

This study seeks to explain the state of the art of deploying cyber volunteers to assist with cybersecurity, the various current organizational structures, the pros and cons of each, attendant legal principles and other issues and measures. We have also examined the limited legislation on this topic because indemnification or legal immunities for good (cyber) Samaritans are critical to preventing the sort of claims and lawsuits that can stifle volunteering efforts. From others' experience and lessons learned, we have endeavored also to make recommendations on how to create and maintain a robust multi-pronged cyber volunteer force in the current environment and into the future. Additionally, we have sought to continue the conversation begun by others and bring the literature on this topic together in one place. We proceed as follows:

[19] Senate Report 117-97 at 2, "Report of the Committee on Homeland Security and Governmental Affairs, to accompany S.1324." August 2022. (https://www.congress.gov/117/crpt/srpt97/CRPT-117srpt97.pdf). This report accompanied the Civilian Cybersecurity Reserve Act, discussed in Section VI.5. *See also* Government Accountability Office*, High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures (GAO-03-121),* at 14 (2003) (www.gao.gov/assets/gao-03-121.pdf).

1. We will review the history of cyber volunteer efforts, including government efforts to establish capabilities through various programs and initiatives along with private responses and efforts.
2. We will discuss the purposes and uses of cyber volunteers primarily around two types of efforts, proactive cybersecurity assessments and reactive incident response. Defending against modern cyber threats requires running a mature information security program that is tailored to the devices and data used by each company. We know that defensive coordination can reduce the likelihood if not the damage of such attacks.
3. We will examine the legal issues, frameworks and infrastructure needed to support cybersecurity volunteering, including the legal and regulatory considerations that must be taken into account when establishing and operating a program.
4. We will evaluate the various models that have been advanced for cybersecurity volunteering, including nonprofit, corporate-backed, university consortium, state-based and federal models, as well as the roles and responsibilities of volunteers and the types of tasks they are expected to perform. We will also address the benefits and drawbacks of each model, including insights into the challenges and successes of existing programs.
5. We will examine the existing support and collaboration mechanisms for cybersecurity volunteers, including licensing, technology and platforms used to facilitate collaboration between organizations.

CHALLENGES OF CYBER VOLUNTEERING

There are a number of practical and legal issues that organizations need to consider when organizing cybersecurity volunteer efforts. Some of the key issues include:

- **Identifying potential beneficiaries or recipients of services**: This can involve a range of practical issues, such as reaching out to or attracting beneficiaries and matching them with volunteers who have appropriate skills and resources to assist.
- **Identifying scope of efforts**: This involves determining a realistic scope of services and other capabilities necessary to address the beneficiaries' cyber needs. This typically includes some sort of proactive assessment work or reactive services such as incident response.

- **Recruitment and vetting**: Recruiting and vetting volunteers can be challenging, and organizations need to consider how to incentivize people to participate. There are also legal issues to consider, such as establishing appropriate liability precautions and indemnity protections for donating companies, the beneficiaries and the individual cyber volunteers.
- **Technical resources**: Obtaining, licensing and using technical resources such as software tools can be a practical challenge, particularly if the organization needs to pay for licenses. There may also be legal issues to consider, such as the terms of use for the tools and any potential liability for their use.
- **Funding**: Sustaining a cybersecurity volunteer effort can be difficult, and organizations may need to consider funding sources such as grants from government or private donors. There may also be legal issues to consider when seeking funding, such as compliance with procurement laws and reporting requirements.

By addressing these practical and legal issues, organizations can more effectively organize and sustain cybersecurity volunteer efforts.

III. HISTORY AND DEVELOPMENT OF CYBER VOLUNTEERING

The concept of cyber volunteering discussed throughout this study can be said to stem from FEMA's NET Guard program promoted by Senator Ron Wyden of Oregon[20] and codified in Section 224 of the Homeland Security Act of 2002.[21] This section "authorized the establishment of a national technology guard comprised of 'local teams of volunteers with expertise in relevant areas of science and technology, to assist local communities to respond and recover from attacks on information systems and communications networks.'"[22] This definition of a cyber volunteer has three important parts: they are **volunteers**, they have **expertise** in computer science or applied cybersecurity and they **assist with response or recovery** following an information system attack. To these, we add that a cyber

[20] Liane Hansen & Sen. Ron Wyden, *NETGuard: High-Tech Volunteers to the Rescue?* (2008) (https://www.npr.org/templates/story/story.php?storyId=92008366).

[21] Homeland Security Act of 2002, Pub. L. No. 107–296, § 224 (2002).

[22] NGA Report at 7.

volunteer may also assist with **preventive action** prior to attacks, but many cyber volunteering efforts have aimed solely at response or recovery.

Ironically, it was Estonia's reaction to Russian cyber attacks that led to some of the federal initiatives in the United States. A wave of cyber attacks in 2007 against Estonia prompted its 2010 creation of a "voluntary Cyber Defence Unit…made up of average citizens outside of government who are specialists in key cyber-security positions, patriotic individuals with information technology skills, and experts in other fields (*e.g.*, lawyers and economists) who wish to volunteer outside of their daily jobs to protect Estonian cyberspace."[23] Estonia's national, quasi-military initiative led to a series of publications that considered whether the United States could benefit from a similar program.[24]

In 2008, FEMA used NET Guard to solicit bids and award $320,000 to four urban areas to pilot cyber volunteering programs.[25] NET Guard was not renewed, and "proponents say the program was never adequately funded and suffered from a lack of interest within the Department of Homeland Security."[26]

In 2013, the commander of US Cyber Command, General Keith B. Alexander, stated he and his team were considering how to involve the national guard of various states to supplement the Cyber Command mission.[27] The resulting efforts were characterized as more "cyber" than "volunteer," as "this effort centers on increasing military capability, lacking societal engagement and offering no way of integrating private-sector talent."[28] Since then, active and ongoing outreach efforts by CISA's Joint Cyber Defense Collaborative (JCDC) have been instrumental in assuaging these concerns, including from some potential cyber volunteers suspicious or distrustful of the federal government. Among other things, CISA senior leadership and JCDC held several in-person, informative sessions at DEF

[23] Bruce Sterling, *Estonian Cyber Security* (2018) (https://www.wired.com/beyond-the-beyond/2018/01/estonian-cyber-security/).

[24] Monica Ruiz, *Is Estonia's Approach to Cyber Defense Feasible in the United States?* (2018) (https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/).

[25] $80,000 each was given to the following cities: "the city of Austin, TX (in the Austin, TX Urban Area Security Initiative (UASI); the city of Chesapeake, VA (in the Norfolk, VA UASI); Cottonwood Heights City, UT (in the Salt Lake, UT UASI); and Hamilton County, IN (in the Indianapolis, IN UASI)." *See* FEMA, *FEMA Announces Awards to Pilot Citizen Corps National Emergency Technology Guard (Net Guard) Program* (2008) (https://web.archive.org/web/20080918062718/http://www.fema.gov/news/newsrelease.fema?id=45806).

[26] Gerry Smith, *The Nerd Reserves: Sandy Recovery Renews Call For Tech National Guard* (2012) (https://www.huffpost.com/entry/tech-national-guard_n_2168374).

[27] United States Senate Committee on Armed Services, *Full Committee Hearing: U.S. Strategic Command and U.S. Cyber Command* (2013) (https://www.armed-services.senate.gov/hearings/oversight-us-strategic-command-and-us-cyber-command).

[28] Ruiz, *supra*, note 24.

CON 30 in the summer of 2022 in Las Vegas, which were well attended and positively received by active participants.

Several publications and organizations have pushed for more widespread and better coordinated cyber volunteering initiatives. The most comprehensive examination of the field to date occurred in 2018, when two publications advocated for a cyber civil defense force: *Task & Purpose* published “We Need A Cybersecurity Awareness Campaign And Civil Defense Force,”[29]and *New America* published “The Need for C3: A Proposal for a United States Cybersecurity Civilian Corps.”[30] These papers laid out an expansion of military-adjacent cyber volunteering efforts under the Department of Homeland Security.

Several nonprofits participate in the cyber volunteering space in a variety of ways. In the United States, Rarenet (Rapid Response Network) has created CiviCERT, “a network of Computer Emergency Response Teams (CERTs), Rapid Response teams, and independent Internet Content and Service Providers who help the civil society prevent and address digital security issues.”[31] CiviCERT is an umbrella organization of civil society actors voluntarily sharing information on incidents. The Center for Digital Resilience provides open-source software tools, information analysis and community engagement.[32] The CTI League, formed during the COVID-19 pandemic, includes numerous volunteers who “protect medical organizations, public healthcare facilities, and emergency organizations from threats from the cyber domain.”[33] Organizations that have paid staff and provide free services include Access Now's Digital Security Helpline[34] and the Cybercrime Support Network,[35] both of which are aimed at individuals.[36]

[29] Jennifer Cruickshank & Iain Cruickshank, *We Need A Cybersecurity Awareness Campaign And Civil Defense Force* (2018) (https://taskandpurpose.com/news/we-need-a-cybersecurity-awareness-campaign-and-civil-defense-force/).

[30] Natasha Cohen & Peter Warren Singer, *The Need for C3: A Proposal for a United States Cybersecurity Civilian Corps* (2018) (https://www.newamerica.org/cybersecurity-initiative/reports/need-c3/).

[31] CiviCERT, Computer Incident Response Center for Civil Society. (2022, Dec 19).

[32] Center for Digital Resilience. (2022, Dec 19). *Center for Digital Resilience Value Pillars*..

[33] CTI-League (https://cti-league.com/) (last visited, Jan. 31, 2023).

[34] AccessNow’s helpline offers support in multiple languages. *See* AccessNow Digital Security Helpline (https://www.accessnow.org/help/?ignorelocale) (last visited, Jan. 21, 2023).

[35] Fight Cybercrime (https://fightcybercrime.org//) (last visited, Jan. 21, 2023).

[36] We also include organizations which pay their own staff to provide free cybersecurity services to others in our definition of a cyber volunteering organization, as they fill the same effective role as those whose staff are unpaid.

There are a number of international efforts toward cyber volunteering that are in some ways more developed than US initiatives. In 2019, international nongovernmental organization (NGO) CyberPeace Institute founded CyberPeace Builders,[37] an effort to help protect other NGOs through cyber volunteering.[38] Other successful cyber volunteering initiatives in the European Union include the France's cyber defense reserves[39] and the pioneering Estonian Defence League's Cyber Unit.[40] The French Cyber Reserve employs cyber volunteers as a component of overall French cyber strategy, which is discussed at length in the *War on the Rocks* commentary "A Close Look at France's New Military Cyber Strategy."[41]

The UK's Cyber Helpline is focused on individual security and uses AI to answer basic questions about cybersecurity, with trained volunteers to take over at need.[42] EU CyberNet, with a similar mission to CyberPeace Builders, is a relatively new offering in this space that provides volunteer expertise to non-EU countries to build cyber capacity.[43] In the worst-case scenario of military-grade cyber attacks, the IT Army of Ukraine[44] operates using crowdfunding and volunteer efforts. Its successes and controversies are discussed in *POLITICO*'s "Kyiv's hackers seize their wartime moment."[45]

More information on nonprofits and others participating in the cyber volunteering space can be found in Appendix 1.

There is also a new generation of university cyber clinics that provide cybersecurity assistance without fees.[46] Many of these clinics are members of the international

[37] Greater Geneva Bern area, *Geneva Welcomes the CyberPeace Institute* (2019) (https://www.ggba-switzerland.ch/geneva-welcomes-the-cyberpeace-institute/).

[38] CyberPeace Institute., *supra*, note 7.

[39] French Cyber Defense Command (https://www.gouvernement.fr/risques/les-reserves-de-cyberdefense) (last visited, Jan. 21, 2023).

[40] Estonian Defense League's Cyber Unit (https://www.kaitseliit.ee/en/cyber-unit) (last visited, Jan. 21, 2023).

[41] *See A Close Look at* France's *New Military Cyber Strategy* (https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/) (last visited Jan. 22, 2023).

[42] The Victim Advice Line (https://victimadviceline.org.uk/specialist-service/the-cyber-helpline//) (last visited, Jan. 21, 2023).

[43] EU Cybernet, *EU CyberNet – the bridge to cybersecurity expertise in the European Union*. (2023) (https://www.eucybernet.eu/).

[44] IT Army of Ukraine (https://itarmy.com.ua/?lang=en) (last visited Jan. 31, 2023).

[45] *See Kyiv's hackers seize their wartime moment* (https://www.politico.eu/article/kyiv-cyber-firm-state-backed-hacking-group/) (last visited Jan. 31, 2023).

[46] Chuck Kapelke. *Cybersecurity Clinics Create Online Defense for the Public Good* (2022) (https://www.newamerica.org/the-thread/cybersecurity-clinics-create-online-defense-for-the-public-good/).

Consortium of Cybersecurity Clinics,[47] co-founded by MIT's Cybersecurity Clinic and UC Berkeley's Citizen Clinic[48] using seed funding from New America's Public Interest Technology University Network. the Citizen Clinic and the UC Berkeley Center for Long-Term Cybersecurity examined volunteer networks in some depth in their white paper titled "Digital Safety Technical Assistance at Scale."[49] The director of MIT's Cybersecurity Clinic, Professor Larry Susskind, has published on the topic of municipal and volunteer cybersecurity.[50]

In June 2022, the National Governors Association (NGA) hosted the National Summit on State Cybersecurity, including a panel on cyber volunteering, and published "Re-Envisioning State Cyber Response Capabilities: The Role of Volunteers in Strengthening Our Systems."[51] This comprehensive report examines state-based cyber volunteering efforts with a focus on Michigan, Wisconsin and Ohio, all of which have relatively sophisticated cyber volunteer programs. The private-sector volunteers who participate in these programs are generally incorporated into the National Guard or state emergency services.

In the for-profit sector, several entities have offered their computer emergency response teams (CERTs) for more general use. Dragos, a threat intelligence and operational tool provider in the cybersecurity space, recently launched its Operational Technology – Cyber Emergency Readiness Team (OT-CERT) to offer "free assessments, recommendations and other cybersecurity resources online."[52] Additionally, the CrowdStrike Foundation offers skill-building opportunities, pro

[47] Consortium of Cybersecurity Clinics (https://cybersecurityclinics.org/) (last visited, Jan. 22, 2023).

[48] *See* MIT Cybersecurity Clinic (https://urbancyberdefense.mit.edu/CybersecurityClinic) (last visited, Jan. 22, 2023). Other cofounders and members of the Consortium include: The University of Alabama Cybersecurity Clinic (https://ida.culverhouse.ua.edu/initiatives/cyber/), the University of Georgia's CyberArch initiative (https://cyberarch.uga.edu/), The Global Cyber Alliance (GCA) (https://www.globalcyberalliance.org/), the Rochester Institute of Technology (https://www.rit.edu/study/computing-security-bs), R Street (https://www.rstreet.org/issue/cybersecurity-and-emerging-threats/), Bina Nusantara University (BINUS) (https://binus.ac.id/), Stillman College (https://catalog.stillman.edu/department-of-computational-and-information-sciences), Columbia SIPA's Capstone Workshops (https://www.sipa.columbia.edu/capstone-workshops/info-clients), and the University of Nevada, Las Vegas Free Cyber Clinic (https://www.unlv.edu/about/highlights/free-cyber-clinic) (last visited, Jan. 22, 2023).

[49] Sean Brooks, *Digital Safety Technical Assistance at Scale* (2020) (https://cltc.berkeley.edu/wp-content/uploads/2020/06/Digital_Safety_Technical_Assistance_at_Scale.pdf).

[50] *See, e.g.,* Benjamin Preis & Lawrence Susskind (2020) (https://doi.org/10.1177/1078087420973760); Gregory Falco, Alicia Noriega & Lawrence Susskind, *Cyber negotiation: a cyber risk management approach to defend urban critical infrastructure from cyberattacks* (2019) (https://www.tandfonline.com/doi/full/10.1080/23738871.2019.1586969).

[51] NGA Report, *supra*, note 8.

[52] Kim Nash, *Tech and Manufacturing Firms Launch Industrial Cybersecurity Group* (2022) (https://www.wsj.com/articles/tech-and-manufacturing-firms-launch-industrial-cybersecurity-group-11654596000).

bono security software and volunteer opportunities for CrowdStrike employees.[53] Other for-profit organizations that have offered free or state-funded cybersecurity services include Synack,[54] HackerOne[55] and Bugcrowd.[56] These three companies participated in bug bounty programs run by the US Department of Defense (DOD).[57]

Notably, in 2022, well-known tech philanthropist Craig Newmark announced that his organization would offer "more than $50 million in grants to build what he calls a 'cyber civil defense.'"[58] The grants are managed by the Aspen Institute's Aspen Digital program, which has already hosted virtual meetings on the topic with a host of participants from nonprofits, government and private industry, including some authors of this study. Aspen Digital is evaluating current models and shared challenges in providing no or low-cost cybersecurity services, as well as monitoring trends and emerging issues.

IV. USES OF CYBER VOLUNTEERS

In this section we will examine the two main uses of cyber volunteers: cyber assessment and incident response. Cyber volunteering programs in the United States have largely sought to use cybersecurity personnel from the private sector as volunteers for high-profile computer emergency response roles, often in CERTs. If cyber incidents are likened to fires, these are the volunteer firefighter teams who respond to these fires.[59] Other programs seek to employ volunteers for assessment and mitigation activities. These volunteers are more like fire code inspectors: they prevent cyber incidents from occurring at all by assisting with compliance using clearly established guidelines.

[53] CrowdStrike Foundation (https://www.crowdstrike.com/about/environmental-social-governance/protecting-our-future/) (last visited, Jan. 22, 2023).

[54] Taylor Hatmaker, *Synack is the latest cybersecurity company to offer state elections its services for free* (2018) (https://techcrunch.com/2018/06/06/synack-election-security-states/). *See also*, Synack (https://www.synack.com/company/) (last visited, Jan. 22, 2023).

[55] *See* HackerOne (https://www.hackerone.com/) (last visited, Jan. 22, 2023).

[56] *See* Bugcrowd (https://www.bugcrowd.com/) (last visited, Jan. 22, 2023).

[57] Sean Michael Kerner, *US Department of Defense Expands Bug Bounty Efforts* (2018) (https://www.eweek.com/security/us-department-of-defense-expands-bug-bounty-efforts/).

[58] Dina Temple-Raston & Will Jarvis, *'A nerd's gotta do what a nerd's gotta do:' Why Craig Newmark is funding a cyber civil defense* (2022) (https://therecord.media/a-nerds-gotta-do-what-a-nerds-gotta-do-why-craig-newmark-is-funding-a-cyber-civil-defense/).

[59] NGA Report at 7.

ASSESSMENT/PREVENTION

Many organizations offer a variety of cyber assessment services, under different models, to beneficiaries. These include assessment against industry frameworks (such as ISO 27001 and the NIST Cybersecurity Framework) or more technical assessments (including vulnerability assessments and penetration testing). Volunteer cybersecurity assessments can be a valuable tool for organizations seeking to improve their cybersecurity posture and better protect against cyber threats.

CISA has collected a variety of resources to assist with assessment and prevention,[60] including free vulnerability scanning services. CISA acts as a critical hub in this space, collating resources to:

- Reduce the likelihood of a damaging cyber incident
- Take steps to quickly detect a potential intrusion
- Ensure that the organization is prepared to respond if an intrusion occurs
- Maximize the organization's resilience to a destructive cyber incident

Further, CISA offers Cyber Hygiene Vulnerability Scanning,[61] though this program is known to currently have long lead times.

By using volunteers for cybersecurity assessments, organizations can tap into a wider pool of resources, including individuals with specialized skills and expertise that may not be available in-house. Additionally, using volunteers for cybersecurity assessments can be more cost-effective than hiring full-time staff or contracting with third-party organizations. Overall, volunteer cybersecurity assessments can help organizations better understand their cybersecurity risks and take steps to mitigate them, ultimately helping to protect against cyber threats.

Key things to consider for volunteer cybersecurity assessments include the following:

- **Expertise**: Cyber volunteers need the necessary expertise to match the type of assessment required for an organization's cybersecurity defenses.

[60] CISA, *Free Cybersecurity Services and Tools* (https://www.cisa.gov/free-cybersecurity-services-and-tools) (last visited, Jan. 22, 2023).

[61] CISA, *Cyber Hygiene Services* (https://www.cisa.gov/cyber-hygiene-services) (last visited, Jan. 22, 2023).

For example, different skillsets are needed to complete a penetration test versus conducting management interviews regarding the NIST Cybersecurity Framework. Depending on the assessment, these skills could include knowledge of cybersecurity best practices, familiarity with a wide range of cybersecurity tools and technologies, and the ability to identify and analyze vulnerabilities.

- **Scope**: The scope of the assessment should be clearly defined in advance, including the areas that the volunteers will focus on and the methods they will use to conduct the assessment. The scope should identify the people, processes or technology that needs to be evaluated and the methodology for the evaluation (such as interview, technical examination and/or testing).
- **Communication**: Effective communication is key to the success of any volunteer cybersecurity assessment. This may include regular progress updates as well as clear and timely communication of any issues or concerns that arise.
- **Recommendations to beneficiary**: Ultimately, recommendations should be provided in a collaborative process giving the beneficiary the opportunity to review and respond as appropriate.
- **Follow-up**: Once the assessment is complete, it is important to follow up on any recommendations or action items that arise from the assessment. This may include implementing new cybersecurity controls, updating existing controls or providing additional training and education to staff.
- **Independence**: The volunteers conducting the assessment typically will be independent because they are not part of the beneficiary organization. This may require matching volunteers who are not affiliated with the organization being assessed.
- **Confidentiality**: The confidentiality of the assessment process should be carefully managed to protect sensitive information and maintain the trust of the organization being assessed. This may include implementing strict confidentiality agreements or using secure communication channels.
- **Legal considerations**: In addition to consents and authorization required to avoid liability under the Computer Fraud and Abuse Act of 1986 (CFAA), Electronic Communications Privacy Act of 1986 (ECPA) and state wiretap statutes, there may be legal considerations involved in the

use of volunteers for cybersecurity assessments, depending on the jurisdiction and the terms of the assessment. It is important to carefully review any relevant laws or regulations to ensure that the assessment is conducted in compliance with all applicable legal requirements.

- **Training**: In order to ensure that the volunteers conducting the assessment have the necessary skills and knowledge, it may be necessary to provide training or other forms of support. This may include providing access to relevant training materials or offering coaching and mentorship to help volunteers develop their skills.

By carefully planning and managing the assessment process, organizations can ensure that the assessment is conducted efficiently and effectively, resulting in meaningful and actionable recommendations for improving cybersecurity.

INCIDENT RESPONSE

State-sponsored cyber volunteering programs focus on building capabilities to respond to large-scale cyber events, including restoration and remediation. Certain clinics and other programs also offer incident response assistance. Most of the literature on cyber volunteering derives from these IR-focused programs, giving the impression that cybersecurity volunteering is primarily for incident response. Incident response is a well-known area of cybersecurity that requires only a small team whose members can be carefully vetted.

That said, it can be a struggle to involve volunteers in incident response, often for the same reasons they are useful. Mainly, specialists in incident response are among the most highly sought-after cybersecurity experts and will have existing professional responsibilities in the event of a broadly targeted cyber attack that may preclude them from being available as volunteers.

The key issues are largely the same as with cyber assessments, with these notable differences:

- **Expertise**: Volunteers must be familiar with working an active cybersecurity breach, including forensic examinations, containment, evidence preservation, recovery, working with counsel under privilege and other skills that are unique to incident response.
- **Scope**: Specific forensic scopes need to be developed that include gathering and analyzing forensic images, threat hunting, dark web

searches, log gathering and analysis, and other common techniques used to actively respond and remediate.

- **Complexity**: Assessment is easier to train for, as incident response can be very complex and high-stress, often requiring around-the-clock support from the incident response team. In contrast, assessment can be performed asynchronously and on the beneficiary's timeframe.
- **Methodology**: Tools necessary for assessment are very different from the forensics suites required for effective incident response. Assessments can often be accomplished through interviews alone, while modern incident response requires a suite of forensics licenses for analyzing logs, data and attackers.

V. LEGAL FRAMEWORKS FOR CYBER VOLUNTEERING

LEGAL ISSUES IN VOLUNTARY CYBERSECURITY ACTIVITIES

There are a number of legal considerations that may be relevant to cybersecurity volunteering, including contractual obligations, data protection laws, privacy laws and intellectual property laws. It is important to ensure that volunteers are operating in a manner that complies with these obligations, as well as any relevant state or federal laws. Both the federal government and states have laws that may be applicable to cybersecurity volunteering, depending on the nature of the work and the location of the volunteers. By discussing the legal considerations involved in cybersecurity volunteering, organizations can ensure that their volunteers are operating in a manner that is compliant with the law and that their activities do not pose a risk to the organization or its clients.

For example, clear authorizations and consent are necessary for volunteers to be able to access a beneficiary's systems and processes, preferably in writing or some type of agreement. The CFAA is a federal law[62] that prohibits unauthorized access

[62] Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030. In May 2022, the US Department of Justice (DOJ) announced an updated policy directing that good-faith security research not be charged under the CFAA. The DOJ will not charge activity that (i) involves accessing a computer solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability; (ii) is carried out in a manner designed to avoid any harm to individuals or the public; (iii) and the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines or online services to which the accessed computer belongs, or those who use such devices, machines or online services. U.S. Dep't of Justice Revised Policy on Charging Violations of the CFAA (May 19, 2022), available at (https://www.justice.gov/opa/press-release/file/1507126/download). This was an effort to "promote privacy and cybersecurity by upholding the legal

to computer systems. It also includes provisions against trafficking in passwords, damaging computer systems, executing a fraudulent scheme using a computer and obtaining sensitive information through computer-related fraud. The ECPA[63] regulates the interception of electronic communications and prohibits such actions without the consent of at least one party involved, with certain exceptions. In the realm of cybersecurity, these laws play a crucial role in protecting computer systems and electronic communications from unauthorized access and interference.

Similarly, many states have wiretap statutes that require one or both parties to consent to access to electronic communications.[64] There are other state laws, in states such as California,[65] Florida,[66] New York,[67] Texas,[68] and Virginia,[69] which criminalize similar activities and aim to safeguard the integrity of computer systems and electronic communications within their jurisdictions.

Many states have initiatives supporting the involvement of cyber volunteers in their cybersecurity efforts, and we have included a listing of such programs in Appendix 2. In this section, we seek to compare some of the variations in these implementations.

Another important consideration is the distinction among a volunteer, an employee and an independent contractor. Generally speaking, volunteers provide their services and time to an organization without payment. As we discuss further below, the relationship with a volunteer needs to be appropriately scoped to avoid creating an employment relationship. A written agreement is one way to formalize the relationship between a cyber volunteer and other parties. See Appendix 3 for a model agreement.

right of individuals, network owners, operators, and other persons to ensure the confidentiality, integrity, and availability of information stored in their information systems." *Id.*

[63] Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522. *See also*, Stored Communications Act (SCA), 18 U.S.C. Chapter 121 §§ 2701–2712 (2021).

[64] *See* Recording Calls and Conversations (https://www.justia.com/documents/50-state-surveys-recording-calls-and-conversations.pdf) for a breakdown of wiretap statutes and their consent requirements across all 50 states. *See also* Reporters Committee for the Freedom of the Press, *Reporter's Recording Guide* (one-party and two-party consent laws under the state wiretap laws) (https://www.rcfp.org/reporters-recording-guide/) (last visited, Jan. 22, 2023).

[65] Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502.

[66] Florida's Computer Crimes Act, Fla. Stat. § 815.06.

[67] New York's Computer Crime and Data Security Law, NY Penal Law 156.05. *See also*, N.Y. Gen. Bus. Law § 899-aa.

[68] Texas' Computer Crimes Law, Tex. Penal Code § 33.01.

[69] Virginia's Computer Crimes Act, Va. Code Ann. § 18.2-152.3.

Finally, although it is not within the scope of this study, it is valuable to consider directly reporting vulnerabilities to CISA, as well as to the vulnerability disclosure programs of various organizations and paid bug bounty programs. The various vulnerability disclosure options allow organizations to accept or offer volunteer cybersecurity assistance in identifying risks before they are exploited, and each has unique practical and legal considerations. We discuss these disclosure scenarios and their implications for the cyber volunteering ecosystem in Appendix 4.

MODEL LIABILITY AND INDEMNITY PROTECTIONS FOR VOLUNTEERS, RECIPIENTS, BENEFICIARIES AND DONORS

Organizations looking to use volunteer help to tackle various cybersecurity issues should consider creating a contractual relationship prior to engaging cyber volunteers. A volunteer agreement is a straightforward way of setting the expectations, formalizing essential information and protecting important interests. Volunteer agreements may include various provisions, depending on the nature of assistance and the relationship, but there are certain provisions that can be viewed as baseline. In addition, each party has its own interests that should be protected through such agreements.

There are at least two parties involved in the provision of cyber volunteer services: a volunteer who is performing cybersecurity services and a beneficiary of those services. This relationship may also include a donor that donates the volunteer services of its workforce and a coordinator that sources the volunteer services and manages the relationship among the volunteer, beneficiary and donor, if applicable.

To define the relationship among the parties and describe the nature of the volunteer services, below is a list of high-level considerations for drafting a cyber volunteer agreement in the United States:

- Include a statement of work that describes volunteer activities.
- Describe the relationship between or among the parties and disclaim any employment relationship between the volunteer and beneficiary.
- Include the beneficiary's consent and authorization permitting the volunteer to access the beneficiary's systems and equipment, as required by the CFAA, the ECPA and the state law equivalents.
- Require confidentiality between or among the parties.
- Include a release and waiver of liability (mutual or one-party).

- Include an indemnification provision (mutual or one-party), under which the parties agree to indemnifications for losses incurred due to the volunteer services.

The above considerations do not represent all provisions that should be negotiated. To assist with drafting a cyber volunteer agreement, Appendix 3 provides a detailed checklist of key provisions and a cyber volunteer model agreement with accompanying instructions. Signed cyber volunteer agreements should be maintained according to existing recordkeeping standards and in compliance with any applicable laws and regulations.

STATE CYBER VOLUNTEERING LAWS

State cybersecurity reserve initiatives, like Michigan's Cyber Civilian Corps Act, aim to improve cybersecurity in a particular state by recruiting and training volunteers to assist with cybersecurity-related activities.

State legal approaches come in basically three forms:

1. Michigan’s comprehensive legislation governing such activities includes provisions for explicit indemnification, an activation mechanism and volunteer accreditation and specifies when the state may offer legal defenses to cyber volunteers.[70]
2. The Texas approach authorizes cyber volunteer activities and their activation but does not include indemnification or accreditation.[71]
3. Louisiana’s approach and proposed legislation in Virginia establish grounds for volunteers to assist without specifying an activation mechanism or other legal protections.[72]

In Appendix 2, we detail the current state and federal initiatives and legal frameworks that enable cyber volunteering. The table includes information about the state or organization running the initiative; the purpose of the program; the state's definition of a volunteer; the activation mechanism for the initiative; and the

[70] Michigan Senate. "Cyber Civilian Corps Act. Act 132 of 2017." *Michigan Legislature.* Jan 24, 2018. (https://www.legislature.mi.gov/documents/mcl/pdf/mcl-Act-132-of-2017.pdf).

[71] *See* TX Govt Code § 2054.52001 et seq (2021).

[72] *See* Virginia Proposed Legislation 2022 Va. Acts H.B. 466 (https://lis.virginia.gov/cgi-bin/legp604.exe?221+cab+HC10202HB0466) ; LA. Stat. Ann. § RS 29:735.4 (2018).

legal indemnities, limitations on protections and legal services provided to volunteers as part of their participation.

These initiatives typically involve the formation of a reserve or corps of volunteers who are trained in cybersecurity and can be activated to assist with responding to cyber incidents, providing cybersecurity training and education, and promoting cybersecurity awareness. State cybersecurity reserve efforts may be established and run by state governments, federal agencies or other organizations and may be supported by legislation or other legal frameworks. Key factors to consider when it comes to state cybersecurity reserve efforts include the following:

- Activation mechanisms may vary, with some initiatives activated in response to specific cyber incidents, while others may be activated on a more continuous basis to support ongoing cybersecurity efforts.
- Training and education are typically important components of state cybersecurity reserve efforts, with volunteers receiving training in areas such as cybersecurity best practices, incident response and digital forensics.
- Legal protections may also be provided, such as indemnification or liability protection, to encourage participation and reduce barriers to entry.
- Collaboration with other organizations and agencies is often an important aspect of state cybersecurity reserve efforts, as it allows for the leveraging of the skills and resources of multiple state agencies, resources and fusion centers to improve cybersecurity and respond to cyber threats.

VI. MODELS FOR COLLABORATION AND PROMOTION OF CYBER VOLUNTEER SERVICES

NONPROFIT MODEL

Description of Model

The nonprofit model includes organizations that exist to provide cybersecurity volunteer services to meet a specific mission statement of that organization. These nonprofits typically champion a limited set of beneficiaries. They may have a statewide, national or even international focus on a particular industry, beneficiary group or charitable cause. Of all the groups, nonprofit organizations may have the most variability because they are not constrained by other bodies (such as state legislatures or other institutions) as to the scope of their mission statements and the beneficiaries that they seek out.

Benefits

The nonprofit model has several benefits, including working nationally; focusing on altruism, which can allow for greater access to beneficiaries through a focused mission; scaling with appropriate funding and expertise; the ability to be run by a variety of actors who can improve connections across industries; and a lack of conflict with a larger parent organization that may impair its missions. However, nonprofits may have obligations to donors which may influence their missions.

First, a nonprofit can work nationally to accomplish its missions. Unlike models that are supported by a state or local government, a nonprofit is free to provide its services across these boundaries.

Nonprofits can also tailor their mission statements to specific areas based on the missions that they carve out for themselves. For example, the Cybercrime Support Network helps individuals who have been targeted by cybercrime in two specific scenarios: victims of romance scams and members of the US military who have been targeted through cybercrime.[73] The CTI League addresses protection of the medical sector and life-saving organizations from cyber-attacks by supplying reliable information, reducing the level of threat, supporting security departments and neutralizing cyber threats through pro bono cybersecurity services.[74] Access Now's Digital Security Helpline is focused on providing real-time technical assistance for civil society groups and activities; human rights defenders; and journalists, media organizations and bloggers around the world. Sightline Security offers assistance to nonprofits and other mission-based organizations aimed at providing them with cybersecurity confidence.

CyberPeace Builders, a volunteer group organized by the Swiss-based CyberPeace Institute, is focused on protecting NGOs,[75] but its model is potentially adaptable to address small and medium-sized critical infrastructure providers in the United States in the following manner:

[73] Fight Cybercrime, *supra*, note 35.

[74] CTI-League (https://cti-league.com/) (last visited, Jan. 22, 2023).

[75] CyberPeace Institute, *supra,* note 7.

- They approach corporate partners to make donations and allow their skilled cyber employees to donate their time.
- They have analyzed and provided model agreements that they enter into with corporate partners, individual volunteers and the beneficiaries/recipients of their free services.
- They have built an effective and scalable software infrastructure to automate the posting of potential pro bono work/jobs for recipients that is used as a matchmaking service with volunteers.
- They monitor the performance of volunteers and have a feedback loop for recipients.

By approaching corporations to volunteer their employee services, nonprofits can rely on corporate partners to vet individual employee volunteers for appropriate skills, thereby avoiding costly background checks, forms and hiring evaluation processes. Each nonprofit sets up internal rules for how it finds beneficiaries and volunteers and then matches individuals who want to volunteer for cybersecurity services with beneficiaries that align with the mission statement of the nonprofit. This approach allows the nonprofit to build deep expertise to meet an identified need and bring in volunteers with an affinity for its mission statement. This level of focus can make the nonprofit a very useful resource for beneficiaries that share its targeted mission, which may open to doors to additional volunteers and beneficiaries that a broad mission statement wouldn't attract.

Nonprofits can also scale up with appropriate funding and expertise. In the beginning, this growth may be small, but it can increase as the nonprofit is rewarded with grants from benefactors who recognize their work or from additional volunteer effort, also in recognition of the work that is performed. This scaling is also driven by market forces: nonprofits that are successful in accomplishing their mission will tend to attract more benefactors, volunteers and beneficiaries, while those that are less successful will remain small, or perhaps re-evaluate their purpose and shift their focus to find a better mission where they can grow.

Nonprofits can set their own rules of engagement, specify which beneficiaries are eligible and set requirements for their volunteers. This allows for broad or narrow reach as defined by the nonprofit's mission statement.

Drawbacks

Nonprofit organizations are not without their drawbacks, including the limited ability to staff incident response activities, as discussed above. Lack of funds or limited mission statements can make it difficult for nonprofits to scale to a large level, so they may remain niche players in a particular mission area. It can be problematic for nonprofits to retain volunteers and employees because their limited funds may prevent them from paying market rates. Once volunteers have achieved their purpose with the organization (be it training, experience or otherwise), they may choose to pursue their personal goals and desires elsewhere. They may also be motivated by new opportunities that are more lucrative or in different geographic locations.

CORPORATE-BACKED MODEL

Description of Model

There are several cybersecurity-focused companies that have developed volunteering initiatives that complement their corporate mission. These companies establish their volunteer initiatives for a variety of reasons, including philanthropy and synergies with their business strategies. For example, Dragos, a company focused on securing operational technology (OT) in industrial control systems (ICS), has developed an OT-CERT team that provides free cybersecurity resources for the ICS/OT community.[76] Additionally, other cybersecurity companies, such the CrowdStrike Foundation, offer volunteer opportunities for their employees and free software for nonprofit organizations.[77] Still other organizations partner with existing nonprofits to provide volunteer opportunities for their employees. This has been fashioned as a way to reduce turnover from cyber employees.[78]

Benefits

Corporate-backed cyber volunteering has several benefits. First, because many corporate-supported volunteers perform cybersecurity functions in their professional life, they can often offer more cutting-edge expertise. For those volunteers who are recruited into these programs from other occupations and professions, these corporate programs can provide valuable training and experience.

[76] Dragos (https://www.dragos.com/ot-cert/) (last visited, Jan. 22, 2023).

[77] CrowdStrike Foundation, *supra*, note 53.

[78] Catherine Stupp, *Businesses Hope to Cut Cyber Turnover by Encouraging Volunteer Work* (2022) (https://www.wsj.com/articles/businesses-hope-to-cut-cyber-turnover-by-encouraging-volunteer-work-11669229253) (highlighting the CyberPeace Institute’s partnership with corporations).

The synergies between paid corporate work and volunteering can also lead to well-paid advisors who are motivated to improve the corporate volunteer programs. Finally, when volunteers come through a corporate-backed model, they often already have been through background checks, which mitigates risk to beneficiaries who benefit from their volunteer efforts.

Additionally, when backed by corporate resources, volunteering initiatives can be highly scalable and may have access to licensed tools or automation that would allow broader reach.

Drawbacks

While some large cybersecurity companies have set up separate foundations, volunteer efforts are not their primary purpose and may take a back seat to larger business objectives. On the other hand, some companies may view their volunteer services as an avenue to build the commercial brand and ultimately recruit more paying customers. The corporate model may not provide the full range of services, depending on the company's product line or goals. Additionally, companies may be very sensitive to appearances and favor volunteer opportunities with positive optics or higher chances of success.

UNIVERSITY CONSORTIUM MODEL

Description of Model

Several universities have built a cyber volunteer clinic model to train student volunteers to address cybersecurity issues for beneficiaries, similar to medical and law clinics in post-graduate education. These programs attract participants from all fields, including from outside computer science and engineering, who are drawn to the mission of assisting community-based organizations. These programs typically run on a semester-by-semester basis and rotate through new volunteers and beneficiaries each semester. Because the services are provided by students, they are supervised by the faculty and staff of the university who run the program. The university model is educationally motivated and provides a range of possible implementations. Leading clinics, such as the MIT Cybersecurity Clinic[79] and UC Berkeley's Citizen Clinic,[80] have been working to introduce this concept to other universities that have existing IT and cybersecurity expertise in their programs. UC

[79] MIT Department of Urban Studies and Planning (https://dusp.mit.edu/classes/cybersecurity-clinic-0) (last visited, Jan. 22, 2023).

[80] UC Berkley Center for Long-Term Cybersecurity (https://cltc.berkeley.edu/about-us/citizen-clinic/) (last visited, Jan. 22, 2023).

Berkeley and MIT co-founded the Consortium of Cybersecurity Clinics with the goal to expand these programs to universities across the country,[81] and regularly assist institutions around the world with starting up new cybersecurity clinics.

Clinics such as MIT and Berkeley provide the opportunity for students with little to no prior knowledge of cybersecurity concepts to become certified in methods of identifying and assessing public agencies' cybersecurity vulnerabilities .[82] Students in the MIT clinic must complete an eight-hour, self-paced online training course followed by a competency exam to receive certification before working in teams to assist public agencies around the country.[83] UC Berkeley's Citizen Clinic trains students to help civil society organizations build their cybersecurity programs, while other clinics serve a range of clients, from medical centers to small businesses to faith-based nonprofits.[84] Some clinics offer custom, long-term engagements as well as shorter ones.[85] There are also clinics that offer more operational services, such as CyberTrust Massachusetts, affiliated with the MassCyberCenter. This university-based program provides a security operations center (SOC) service to municipalities in Massachusetts.[86]

Benefits

The cybersecurity clinic model has several benefits. First, it has a continuing source of volunteers, including students who are already focused on IT or cybersecurity and mission-oriented students from other major programs. These clinics can offer a valuable service to beneficiaries, as well as to students who want experience in cybersecurity but may struggle to gain an entry-level position without hands-on experience. The clinic model can also help a student who may not be ready to commit to a cybersecurity career understand what is involved and get that first set of experiences. Additionally, clinics can assist a wide range of beneficiaries, similar to the nonprofit models, and can tailor their mission statements to target specific types of beneficiaries that have an affinity to the program.

Many clinics assist local beneficiaries. The results of these efforts can lead to published findings that advance the entire cybersecurity industry by providing case

[81] The Consortium of Cybersecurity Clinics (https://cybersecurityclinics.org/) (last visited, Jan. 31, 2023).

[82] Internet Policy Research Initiative MIT (https://internetpolicy.mit.edu/news-introducing-the-mit-cybersecurity-clinic/) (last visited, Jan. 22, 2023).

[83] MIT Department of Urban Studies and Planning, *supra*, note 79 .

[84] UC Berkeley Center for Long-Term Cybersecurity, *supra*, note 80.

[85] *Id.*

[86] Cyber Trust Center (https://www.cybertrustmass.org/).

studies, after-action reports and academic articles. The model excels at providing an entry point for students who have an interest in cybersecurity and offers valuable initial training and experience with real-world situations. In the long term, clinics also may help create the next generation of IT and cybersecurity staff, which could help offset the current personnel deficit.

Cyber Legal Clinics

Much like existing legal clinics in many law schools, a new program for cyber legal clinics could be developed at leading law schools. These would not be a semester program. Rather, they would last at least through the school year and would have an educational component focused on incident response, data breach notification laws, legal privilege in assessments and forensic reports, with supervision of a practice law professor. These programs would help develop a cadre of lawyers who are familiar with incident response and cyber attack procedures and related legal principles. Much like traditional legal clinics involving low-income legal services, public defender and district attorney programs, these cyber legal clinics would provide hands-on, real-life experience with clients who were victimized by actual or potential attacks. Forensic vendor assistance for cyber volunteers could also be coordinated, potentially with other departments or programs within the university that offer more technical volunteer student clinics.

Drawbacks

One of the biggest issues with the university clinic model is scaling and the need to fit the projects into the semester timeline. A project should ideally start near the beginning of the semester and end when the semester is over to coincide with student availability. This means the clinic model is not well suited for incident response activities that could happen at any time, other than potentially through a law school clinic model. This model is best suited for projects that can be planned in advance, such as prospective assessment work or remediation recommendations. Additionally, with the heavy need for student supervision and the limited capacity of faculty and staff, there are scaling issues with how many projects can be undertaken each semester. Furthermore, much of the time spent on a project is necessarily devoted to training students rather than completing additional projects.

If a project cannot wrap up at the end of a semester, there may be significant delays as new students enter the clinic, undergo training and get up to speed on work that has already been accomplished by prior students. This means assessments that take longer than a semester may not be ideal for the university clinic model.

Additionally, beneficiaries that may need to rely on the clinic for yearly or follow-up assessments do not benefit from the continuity offered by an assessment team that is familiar with the beneficiary and able to bring that knowledge to the next year's assessment.

STATE MODEL

Description of Model

The National Governors Association has careful documentation, analysis and introspection regarding the effectiveness of state-level cyber volunteering programs, providing much of the background used to analyze this topic throughout this study.[87] The state-backed model consists of cyber volunteering initiatives run by a non-federal government entity. Our commentary is based on the volunteer aspects of these programs. These volunteer programs are usually run by the executive branch and placed under the National Guard or Emergency Services.[88] Most state governments currently have a CERT that is staffed with paid professionals. Some states also have a volunteer component, and most could be expected to ask for and receive volunteer assistance from both affected parties and industry professionals in the case of a cyber emergency. Michigan, Wisconsin and Ohio have formalized this volunteer component. The MassCyberCenter focuses on cybersecurity resiliency throughout the Commonwealth of Massachusetts[89] and provides a variety of training, workshops, mentoring and job development services and opportunities.[90]

Generally, state-backed cyber volunteer initiatives must be "activated" like a National Guard unit or SWAT team. The members of some volunteer teams, such as in Ohio, become National Guard or executive-branch employees, with the appropriate legal protections accruing upon activation. They can include municipal and multi-state initiatives, and sometimes have associated legislation. A more in-depth examination of the legal aspects of these state initiatives can be found in Appendix 2 of this study.

In 2013, Michigan took the lead in establishing its Michigan Cyber Civilian Corps (MiC3), "a group of trained, civilian technical experts who individually volunteer to

[87] NGA Report, *supra*, note 8.

[88] We are not addressing here the various organizations or entities involved in state or federal election cybersecurity precautions.

[89] MassCyber Center (https://masscybercenter.org/) (last visited Jan. 22, 2023).

[90] *Id.*

provide rapid response assistance to the State of Michigan in the event of a critical cyber incident."[91] MiC3 incorporates experienced cybersecurity professionals into Michigan's cybersecurity response framework to strengthen the state's network and systems against attackers. The group is comprised of volunteers who are trained experts. MiC3 members have at least two years of direct involvement with information security, possess a basic security certification and can commit up to 10 days per year for training and exercises. In 2017, Michigan passed the Cyber Civilian Corps Act, which supports the MiC3 initiative with legal indemnification for volunteers and made Michigan the de-facto leader in state-backed cyber volunteering initiatives.[92]

Several other states followed suit in creating cyber volunteer programs aligned with state executive offices. They include Wisconsin, Ohio, Indiana, Maryland, Virginia, Texas, Oklahoma, California and Louisiana. Combinations of volunteers and National Guard detachments are regularly involved in incident response for state and municipal organizations. Wisconsin's team has reportedly been deployed in over 30 incidents.

State-backed cyber volunteers in incident response roles can offer mid-tier and small organizations access to remediation capabilities that they otherwise could not afford, and have clear value in training and coordinating state-level emergency response efforts toward cyber scenarios. For a variety of reasons, they have not seen widespread deployment in recent security incidents such as the Log4j vulnerability and SolarWinds hack, but in the event of an industry-specific or localized attack, they could bring great value in coordinating activities alongside FEMA, the National Guard and other emergency efforts.

In order to effectively deploy volunteers and leverage their skills and expertise, state cybersecurity reserve efforts may involve coordinating with other organizations and agencies and establishing protocols for communication and collaboration. Support—including training and education, equipment and supplies, and logistical support—may also be provided to ensure that volunteers are well equipped to assist with cybersecurity-related activities and are able to contribute effectively. Regular evaluation of state cybersecurity reserve efforts is important to identify areas for improvement and optimize the use of volunteers. This may

[91] Michigan Cyber Civilian Corps (MiC3) (https://www.michigan.gov/dtmb/services/cybersecurity/michigan-cyber-civilian-corps-mic3) (last visited Jan. 22, 2023).

[92] Cyber Civilian Corps Act, Act 132 of 2017.

include collecting data on the activities and impact of volunteers, as well as soliciting feedback from volunteers and other stakeholders.

Benefits

Operations under state government offer legal indemnities or immunities not available under other models. As described above, legislation at the state level has been proposed and enacted to provide indemnity, ranging from Virginia's proposed cyber volunteer registry to the broad indemnification provisions in Michigan. Some states may only indemnify formal members of their programs; however, Louisiana and Maryland incorporate cyber volunteers under more general volunteering frameworks, which allow non-state employees to participate. See Appendix 2 for more details.

Of the models we examined, state-backed cyber volunteers are well positioned to interact with critical infrastructure providers for incident response with minimal regulatory concern. The state-backed volunteers have connections and shared goals at a local level, which enable direct action. The state and municipal critical infrastructure organizations that often lack in-house cyber response and remediation capacity are relatively easy for these state-backed cyber volunteers to interact with, as they operate on similar levels.

State-based cyber volunteers, for certain members of the public, have a level of credibility by virtue of their association with their home states, similar to how National Guard operations or firefighters are largely trusted in emergency situations. Accordingly, these cyber volunteers can act with the approval or oversight of state authorities and potentially provide services without other onerous service agreements. However, state-backed cyber volunteers must often sign agreements limiting their operations to those directed by the state services overseeing them.

State-backed cyber volunteer programs require background checks, certifications, training and explicit agreements with their volunteers. States and National Guard units also have access to the resources and personnel to create military-grade training programs and keep their people at a relatively high readiness level.

Drawbacks

Most of the state-backed volunteer models have activation requirements based on state direction. Further, state efforts do not operate outside of state boundaries and would require collaboration arrangements between or among state executive offices.

Another drawback is the sheer variety of potential victims that state organizations might be expected to assist. Everything from municipally based critical infrastructure providers to high-profile individuals in the government or government agencies may fall under the remit of a state cyber incident and require a response. It is difficult to amass the capabilities required to help such a diversity of potential victims. For example, the reactive skills necessary to address and remediate a ransomware attack at a rural municipal hospital are widely divergent from the proactive skills needed for an assessment of the same hospital's basic cybersecurity. The wide range of potential actors in the area also cause other issues. Hospital software remediation and energy-sector SCADA controls, for example, require skillsets that only exist within a small subset of cyber professionals. It may be difficult for states to recruit from within those specialties.

The high costs of vetting, training and maintaining readiness for all state-backed cyber volunteer programs means the programs are not readily scalable. Rather, state initiatives are based on small, highly vetted, highly trained incident response teams with local connections. The state volunteer programs are the most capable volunteer programs to respond to municipal or state issues, but if there is a larger incident even within their states, they may find it challenging to assemble adequate personnel or scale up in the near term. There are few statistics relating to the deployment of volunteer forces by states, although Wisconsin's team is reported to have responded to more than 30 cybersecurity incidents. In part, the dearth of statistics may be because efforts involving volunteers, national guard detachments, fusion centers and other state actors are sometimes conflated for statistical and reporting purposes.

State initiatives may also face budget cuts and hiring slowdowns based on factors such as the COVID-19 pandemic. States may be able to help fill the gaps with contractors, but employing them quickly in response to an incident that necessitates state action requires extensive prior vetting and networking. The need for such connections or contracts is unlikely to be apparent until an attack hits and staffing is deemed insufficient.

State volunteer programs may have a lead time of around six months to turn even top applicants with tech skills into certified cybersecurity professionals, similar to the timeframe the US Air Force applies to its cybersecurity training program that grants a CompTIA Security+ certification.[93] On the other hand, at need, the state program could be scaled up to include all persons with such aptitudes who are already vetted members of emergency or National Guard services. The pool of these state-based volunteers could in some ways exceed those available to other cybersecurity volunteer models.

Due to their reliance on state and primarily executive support, potential political pressures may influence critical factors in state cyber volunteer organizations, including composition, strength, long-term effectiveness and willingness to use the volunteers.

FEDERAL MODEL

In 2008, FEMA's NET Guard launched a pilot program in four major cities, as described earlier in section III. This could be said to constitute the beginnings of a federal program to directly coordinate and employ cyber volunteers. Although there is not much information on the outcomes from this program, its statutory basis still exists, suggesting that with appropriate coordination the program could be resurrected.

Given the lack of information regarding the outcomes of the NET Guard pilot program, we assume that CISA does not wish to engage individuals as volunteers working for the federal government.

Description of Model

Federal-level implementation and coordination of cyber volunteering efforts is nascent, but several pieces of legislation and pilot programs point toward increasing activity in the future. There is also a bill under consideration by the US Congress titled S.1324 – Civilian Cybersecurity Reserve Act. This bill, which passed in the Senate and was sent to the House in December 2022, would allow the director of CISA to appoint selected individuals to a federal Civilian Cybersecurity Reserve, from which up to 30 persons could be activated and become federal civil service employees. Similar to the state-backed initiatives, these persons would be vetted but may not be members of the executive branch. Though a team of 30 people would be not large enough in terms of total volunteers, the design of the program suggests that they could act as coordinators and liaisons who can potentially:

[93] CompTIA Security+, Certification (https://www.comptia.org/certifications/security. “CompTIA Security+ is a global certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career.”) (last visited Jan. 22, 2023).

- Deploy and manage significant numbers of other volunteers
- Provide subject matter expertise
- Grant access to resources otherwise unavailable, for example, if one or more of the 30 were well connected in the cybersecurity industry

Generally speaking, a federal cybersecurity volunteering model is likely to be similar to FEMA. For example, a cyber program might standardize trainings and offer associated credentialling, as is the case with FEMA's Incident Command System. They might also coordinate with FEMA to ensure that its existing training includes modules on cyber attacks and potential fallout.

They might also liaise with the DOD. Though the Civilian Cybersecurity Reserve Act would bar employing current members of the executive branch,[94] it also stipulates that members must have previously served in government, including the military.[95] This builds a platform from which shared language and experiences would allow the cyber reserve or a similar program to interact easily, if not seamlessly, with other parts of the federal government.

Benefits

Unlike state-backed cyber volunteer programs, a federal program can work across state, regional and even national boundaries. Further, a federal initiative can coordinate and draw from National Guard efforts. US Cyber Command has already examined and expressed an interest in this form of activation in the event of a national-scale event.

Federal initiatives can draw on federal funds and resources, including access to military and political tools unavailable to other models. Some examples include using cadres from the US military for training or seeking federal grants under DHS to fund subsidiary programs. The resources available for national defense often dwarf those available elsewhere, even at the state level. Ideally federal volunteer programs can employ national coordination of responses that build upon CISA's remarkable efforts to educate about cyber incidents such as the Log4j vulnerability and the SolarWinds hack. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) shows some of the potential of federal-level cyber volunteer

[94] Civilian Cybersecurity Reserve Act, S. 1324 § 2(c)(7).

[95] *Id.* § 2(c)(2)(A).

indemnification, but additional legislation or action under the executive branch would be necessary for this to be a benefit of federal programs.

Drawbacks

Depending on the implementation, a federal cyber volunteering program may be sensitive to political pressures and limitations under the federal system. For example, presidential elections may have significant consequences. A change in administration at the federal level may be even more pronounced than in the state-backed systems.

Absent a crisis, federal initiatives can be relatively slow-moving and require coordination between branches for maximum effect. Understandably, CISA may be looking to state and nonprofit arenas to more quickly implement some of this guidance and to partner with these entities for more effective near-term results.

VII. OTHER CONSIDERATIONS

LICENSING, TECHNOLOGY AND PLATFORMS

Cybersecurity professionals rely on software applications and platforms for virtually all aspects of proactive and reactive services. For purposes of this study, the technology that cybersecurity professionals leverage can be grouped into three categories:

1. Technology that enables or accelerates cybersecurity assessments and forensic investigations, such as vulnerability scanning tools and forensic analysis toolkits
2. Technology that provides operational cybersecurity, such as antivirus software, firewalls, logging and monitoring solutions, *etc*.
3. The core technologies that enterprises use to conduct their operations, such as office software, communications platforms, ecommerce platforms, operations technology, *etc*.

Either the volunteer organizations or the beneficiaries would need to develop their own software or seek licenses for security software to enable assessments and incident response. Volunteers and the organizations that support them likely would not be able to contribute software licenses for operational cybersecurity technologies out of their own funds. Therefore, licensing becomes an essential challenge to establishing a volunteering organization and providing services to beneficiaries. Additionally, many of these tools require significant expertise to install and maintain and, even if licenses are free, there may be significant costs.

Most commercial assessments and incident responses do not rely solely on free and open-source software (FOSS) tools and instead use commercially available solutions such as Forensic Toolkit (FTK), EnCase, Cobalt Strike and Nessus. If FOSS tools were readily available, this could be a partial solution to the licensing problem. However, the most-used tools in this space are not FOSS; they are either proprietary or free for certain limited uses that might not be applicable to a typical security assessment or engagement.[96] Additionally, the volunteers would likely have less experience with existing FOSS solutions than with proprietary tools because of their prevalence in commercial engagements.

There are at least three possible solutions to this challenge. First, volunteer organizations could develop their own software or negotiate favorable licensing agreements with software producers. Some commercial security software is already available for pro bono efforts.[97] Commercial security software producers are motivated to provide this software for pro bono efforts as a means of enhancing public welfare and supporting their corporate social responsibility goals. Additionally, some software producers might be enticed to contribute free or reduced-cost licenses to volunteer organizations if they believe that use by a volunteer organization could result in the following:

- An increased likelihood that the receiving entity will purchase their products and services for later use
- The volunteers acquiring training and expertise in the tools, thereby increasing the likelihood that they would purchase or recommend the tools in their regular employment capacity

Second, volunteer organizations could leverage existing public resources, such as CISA's Cyber Hygiene Services,[98] which is primarily a vulnerability scanning tool. Although CISA has addressed manpower challenges by adding regional security assistance representatives, the organization reported that it can take weeks to obtain

[96] *See, e.g.*, OWASP, *Vulnerability Scanning Tools* (https://owasp.org/www-community/Vulnerability_Scanning_Tools) (last visited Jan. 22, 2023).

[97] *E.g.*, CrowdStrike, *Pro bono security software* (https://www.crowdstrike.com/about/environmental-social-governance/protecting-our-future/#probono) (last visited Jan. 22, 2023); Justin Spelhaug, *Strengthening cyber defenses for non-profits* (2023) https://blogs.microsoft.com/on-the-issues/2021/10/21/cyber-defenses-security-program-non-profits/; Cloudflare, *Project Galileo* (https://www.cloudflare.com/galileo/) (last visited Jan. 22, 2023).

[98] *Cyber Hygiene Services*, *supra*, note 61.

a penetration test once it has been requested.[99] To the extent that CISA's services or similar public resources are capacity-constrained, trained volunteer organizations could expand the reach of these services. CISA's site also provides a listing of Free Cybersecurity Services and Tools,[100] which includes a variety of tools, websites and solutions. Some are open-source, some are limited products and others are websites. It would take a committed volunteer to go through these various options to build a security program for a beneficiary, and certain tools and solutions on CISA's list may not all be readily available.

Third, the development of robust FOSS security solutions should be encouraged for a long-term option. While this would obviously make for good public policy, it would be beyond the capability of a volunteer organization. Additionally, this will take time to accomplish and will not be available in the short term.

FUNDING AND GRANTS

In September 2022, the Biden-Harris administration announced a first-of-its-kind State and Local Cybersecurity Grant Program, which will provide $1 billion to state, local and territorial government partners (SLTs) over five years, with $185 million already made available in the 2022 fiscal year.[101] The grant program will allow SLTs to address cyber risk in their information systems, strengthen the cybersecurity of their critical infrastructure and increase resilience against persistent cyber threats.[102]

This level of funding over the next four years can have significant consequences on the nation's cybersecurity resilience. However, as the $1 billion, including the $185 million allocated in fiscal year 2022, is being distributed across the whole nation, the amount that each municipality will receive to address its own cybersecurity needs could be less than anticipated. For example, Massachusetts was provided $3 million in the 2022 fiscal year, which the state has to divide across 351 municipalities. If all municipalities were given the same amount, each would receive approximately $8,547 to support its cybersecurity needs. Although the grant program makes great strides in providing the support needed to strengthen

[99] *See CISA Call with Critical Infrastructure Partners on Potential Russian Cyberattacks Against the U.S.* (https://www.youtube.com/watch?v=q-vnMmQHASY) (last viewed Jan. 31, 2023).

[100] *Free Cybersecurity Services and Tools*, *supra*, note 60.

[101] *Biden-Harris Administration Announces $1 Billion in Funding for First-Ever State and Local Cybersecurity Grant Program* (2022) (https://www.dhs.gov/news/2022/09/16/biden-harris-administration-announces-1-billion-funding-first-ever-state-and-local)

[102] *Id.*

cybersecurity, some SLTs may need access to additional funding to fulfill their cybersecurity goals, including undergoing a cyber risk assessment and implementing a basic incident response plan.

VIII. CONCLUSION

Despite more than two decades of attention from lawmakers, philanthropists, academics and scholars, there are potential solutions in the cyber volunteering arena that remain untapped and lightly explored. In particular, there appear to be many qualified individuals who are willing to provide pro bono cybersecurity services. They may be challenged in finding suitable enterprises that need their services and could significantly benefit from platform entities to coordinate the delivery of these volunteer services. This challenge may be due to a number of factors, including the variety of organizations in this space, some of which are siloed. Additionally, the field is not yet well coordinated.

While we have provided a snapshot of pro bono cybersecurity services in this study, we recommend a more holistic undertaking to capture the full breadth of available services. We hope that our more granular recommendations, set out in the Executive Summary and Recommendations section, will help set the stage for further cyber volunteer efforts and a more cyber-secure future.

McDermott
Will & Emery

AUTHORS

MARK E. SCHREIBER
SENIOR COUNSEL
mschreiber@mwe.com
Tel +1 617 535 3982

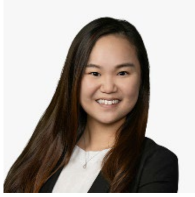
SCOTT FERBER
PARTNER
sferber@mwe.com
Tel +1 202 756 8988

BRIAN LONG
ASSOCIATE
brlong@mwe.com
Tel +1 214 295 8085

PETER SCHEYER
LAW CLERK
pscheyer@mwe.com
Tel +1 202 756 8107

ROBERT DUFFY
COUNSEL
reduffy@mwe.com
Tel +1 202 756 8790

MARINE MARGARYAN
ASSOCIATE
mmargaryan@mwe.com
Tel +1 202 756 8555



CATHY LEE
ASSOCIATE
cjlee@mwe.com
Tel +1 202 756 8141

AMY C. PIMENTEL
PARTNER
apimental@mwe.com
Tel +1 617 535 3948

Appendix 1
List of Nonprofit, Corporate, University and State Cyber Volunteer Organizations

The following descriptions and links to cyber volunteer organizations are current as of the date of this study in March 2023. McDermott Will & Emery LLP does not and cannot vouch for or endorse these organizations, nor can McDermott Will & Emery LLP represent that the information included below is accurate or complete. There may be other organizations that we were not aware of or did not include.

NONPROFITS

Access Now's Digital Security Helpline works with individuals and organizations around the world, providing real-time technical assistance and advice. They use paid personnel to provide free services. The helpline walks individuals and organizations through assessing, prioritizing and remediating cybersecurity risks. The helpline works with civil society groups and activists, media organizations, journalists and bloggers, and human rights defenders. The helpline's services are available 24/7, and support is available in nine languages: English, Spanish, French, German, Portuguese, Russian, Tagalog, Arabic and Italian.

Aspen Digital, a program of The Aspen Institute, provides insight on urgent global issues concerning cybersecurity, information ecosystems, emerging technology, industry talent pipelines, tech and communications policy, and innovation. Aspen Digital develops human solutions to these digital problems through efforts such as the Commission on Information Disorder, the Aspen Cybersecurity Group and the Aspen Tech Policy Hub.

CiviCERT is a network of computer emergency response teams (CERTs), rapid response teams, and independent internet content and service provides, who help civil society prevent and address cybersecurity issues. CiviCERT is an initiative of Rarenet, which is an umbrella organization formed by internet content and service providers, NGOs and other individuals to offer these emergency response services.

CTI League aspires to protect the medical sector and life-saving organizations worldwide from cyber-attacks, supplying reliable information, reducing the level of threat, supporting security departments and neutralizing cyber threats.

The **Cybercrime Support Network** (CSM) provides individuals and organizations with information needed to recognize, report and recover from cybercrime. CSM has information on various scams, such as financial purchase scams, imposter scams and identity theft. They also offer support to peer and veterans support programs.

CyberPeace Builders (CPB) provides free cybersecurity support to NGOs in the humanitarian and development sectors. The CPB are a cohort of experts and volunteers who provide local and tailored support to each NGO partner. To date, they have assisted 101 NGOs operating in 120 countries and have more than 200 volunteers.

CyberTrust Massachusetts funds a 24/7 security operations center (SOC) backbone via a managed security service provider on which students can take a Tier 1 SOC shift.

NONPROFITS LOCATED AND ORIENTED OUTSIDE THE UNITED STATES

Cyber Helpline in the UK uses AI to answer basic questions from individuals about cybersecurity, with trained volunteers to take over as needed.

The **Estonian Defence League's Cyber Unit** employs cyber volunteers and has been a pioneer in the cyber volunteering space since its inception.

EU CyberNet has a similar mission to CyberPeace Builders and provides volunteer expertise to non-EU countries to build cyber capacity.

The French Cyber Reserve employs cyber volunteers. This and the broader French cyber strategy are discussed at length in the *War on the Rocks* commentary "A Close Look at France's New Military Cyber Strategy."[103]

The IT Army of Ukraine operates using crowdfunding and volunteer efforts. Its successes and controversies are discussed in *POLITICO*'s "Kyiv's hackers seize their wartime moment."[104]

COMPANIES

Dragos is putting together a members-only OT-CERT program for owners and operators of small and medium-sized industrial operations that have operational technology (OT) needs. The program is in the beginning stages (as of July 2022), but Dragos plans to roll out several self-service tools, including an OT cybersecurity survey, an OT asset management tool and a basic OT cybersecurity tabletop. The OT-CERT program is not focusing on hands-on assistance, but rather a user group process to allow members to share information.

Synack, **HackerOne** and **Bugcrowd** offer free cyber assistance. These companies participated in DOD-run bug bounty programs, which did not offer an assurance of payment, ran for the public good and operated using cyber volunteering principles. It is unclear if these companies are still running these bug bounty programs. Synack also offered free penetration testing to help secure election machines for the 2018 elections.

UNIVERSITIES

The Consortium of Cybersecurity Clinics is an umbrella organization of university cybersecurity clinics.

The **MIT Cybersecurity Clinic** will provide an opportunity for students to become certified in methods of identifying and assessing public agencies' cybersecurity vulnerabilities. The certification involves completing an eight-hour, self-paced, online training followed by a competency exam. Certified students will then work in teams to assist public agencies around the country with vulnerability assessments.

[103] *See A Close Look at France's New Military Cyber Strategy* (https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/) (last visited Jan. 22, 2023).

[104] *See Kyiv's hackers seize their wartime moment* (https://www.politico.eu/article/kyiv-cyber-firm-state-backed-hacking-group/) (last visited Jan. 31, 2023).

The **UC Berkeley Citizen Clinic** trains law students to help civil society organizations build their cybersecurity programs. Clinic students will help these organizations proactively defend against digital threats, as well as provide trainings on cybersecurity. The clinic also offers custom, long-term engagements.

The Strauss Center at the University of Texas at Austin offers a number of programs targeted at cybersecurity and national security. These programs include the Integrated Cybersecurity Studies program and Intelligence Studies Project. The Strauss Center offers fellowships and other research opportunities to delve into emerging international challenges.

STATE ACTORS

The state programs are discussed in more detail in Casey Dolen's Re-Envisioning State Cyber Response Capabilities: The Role of Volunteers in Strengthening our Systems. Below we have provided a high-level overview.

The **National Governors' Association** (NGA) identified priority issues and dealt with matters of public policy and governance at the state, national and global levels. In 2022, the NGA hosted a National Summit on State Cybersecurity to discuss a wide range of cybersecurity issues affecting the states.

STATE-ORGANIZED CYBER VOLUNTEERING PROGRAMS

The following programs are described in detail in Appendix 2 and the State Model section of the study:

Michigan Cyber Civilian Corps (MiC3)

Michigan Cyber Partners

Texas Volunteer Incident Response Team (VIRT)

Ohio Cyber Reserve (OhCR)

California Cybersecurity Integration Center (Cal-CSIC)/Cyber Incident Response Team

Wisconsin Cyber Response Team (CRT)

Oklahoma Civilian Cyber Corps (OKC3)

Maryland Defense Force (MDDF) Cyber Security Unit (CYSEC)

The Bay Area Urban Areas Security Initiative (UASI)

MassCyberCenter

Appendix 2
Analysis of State and Federal Cyber Volunteering Laws and Efforts

Current as of the date of this study

STATE, AGENCY, LEGAL BASIS	PURPOSE	DEFINITION OF VOLUNTEER	ACTIVATION MECHANISM	INDEMNITY, LIMITATIONS, STATE LEGAL SERVICES
STATES WITH EXISTING STATUTES				
Michigan: Michigan Cyber Civilian Corps (MiC3) Under: Michigan Department of Technology, Management & Budget (DTMB) Code: Mich. Comp. Laws § 18.221-230 Legislation: 2017-PA-0132.pdf (mi.gov) January 24, 2018 (Effective)	“Create a program under which volunteers may provide services to organizations in this state to respond to cybersecurity incidents.” Act 132 of 2017 "Cybersecurity incident" definition requires actual or imminent jeopardy of integrity, confidentiality, or availability. Includes, “but is not limited to, the existence of a vulnerability in an information system, system security procedures, internal controls, or implementation that is subject to exploitation.” (Mich. Comp. Laws 18.222(e))	"Michigan cyber civilian corps volunteer" means an individual who has entered into a volunteer agreement with the department to serve as a deployable volunteer in the Michigan cyber civilian corps. § 18.222(i) “[C]ivilian volunteers who have expertise in addressing cybersecurity incidents may volunteer at the invitation of the department to provide rapid response assistance to a municipal, educational, non-profit, or critical infrastructure organization in need of expert assistance during a cybersecurity incident.” § 18.222(h)	Client undergoes cybersecurity incident, requests volunteer(s), department may initiate deployment. “On the occurrence of a cybersecurity incident that affects a client” Request by client, approval of DTMB, then volunteers can be deployed. Mich. Comp. Laws 18.228	State from volunteer actions, volunteer from tort liability. (Mich. Comp. Laws 18.227(1-2)) Limitations: Must be: 1. “acting or reasonably believe” acting in scope, 2. not grossly negligent, 3. not materially breaching volunteer agreement. Mich. Comp. Laws 18.227(a-c). Volunteer Agreement Contract Provisions: Mich. Comp. Laws 18.224. State Legal Assistance: Civil: Yes, department may provide. Mich. Comp. Laws 18.227(3) Criminal: Department may provide. Mich. Comp. Laws 18.227(4)

STATE, AGENCY, LEGAL BASIS	PURPOSE	DEFINITION OF VOLUNTEER	ACTIVATION MECHANISM	INDEMNITY, LIMITATIONS, STATE LEGAL SERVICES
Texas: Texas Volunteer Incident Response Team (VIRT) Under: Texas Department of Information Resources (DIR) Code: TX Govt Code § 2054.52001 et seq (2021) June 14, 2021 (Effective/Passed)	"[P]rovide rapid response assistance to a participating entity under the department's direction during a cybersecurity event." (TX Govt Code § 2054.52002)	"'Volunteer' means an individual who provides rapid response assistance during a cybersecurity event under" activation mechanisms in code. Sec. 2054.52001(3)	A cybersecurity event affects multiple "participating entities" or declaration by the governor of a state of disaster caused by a "cybersecurity event." Department may then deploy volunteers under its direction. Sec. 2054.52005 Cybersecurity event is not defined in Texas code, but Texas Cybersecurity Framework is "aligned" with NIST. "Participating entity" means a state agency, including an institution of higher education, or a local government that receives assistance under this subchapter during a cybersecurity event. Sec. 2054.52001(2) "A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation)." NIST definition from NIST SP 800-160 Vol. 2 Rev. 1	State is not liable to volunteer, volunteer is "not an agent, employee, or independent contractor of this state for any purpose and has no authority to obligate this state to a third party." § 2054.52008 Volunteer is not liable for civil damages, limited to services provided during a cybersecurity incident. § 2054.52009 Limitations: Good faith provision of professional services requirement. Not "willful and wanton misconduct." Immunity is "limited to services provided during the time of deployment for a cybersecurity event." § 2054.52009 State Legal Assistance: Not mentioned.

STATE, AGENCY, LEGAL BASIS	PURPOSE	DEFINITION OF VOLUNTEER	ACTIVATION MECHANISM	INDEMNITY, LIMITATIONS, STATE LEGAL SERVICES
Ohio: Ohio Cyber Reserve Under: Adjutant General's Department, "When called to state active duty by the governor, reserve members shall function as civilian members of the Ohio organized militia." Section 5922.08 - Ohio Revised Code | Ohio Laws January 14, 2020 (Effective)	"[T]o educate and protect state, county, and local government entities, critical infrastructure, including election systems, businesses, and citizens of this state from cyber attacks." Ohio Revised Code § 5922.01 "[A]ssist eligible municipalities with cybersecurity vulnerabilities and provide recommendations to reduce cyber threats. Ohio Cyber Reserve (OhCR) page.	"[C]ivilian cyber security reserve forces capable of being expanded and trained" to achieve purpose as members of National Guard. Ohio Revised Code § 5922.01 Must be qualified. Ohio Revised Code § 5922.05	Must be "ordered out for active service by the governor." Ohio Revised Code § 5922.06	Ohio code of military justice applies.
STATES WITH PROPOSED STATUTES				
Indiana: Indiana Cyber Civilian Corps [NOT PASSED] Under: Indiana Department of Administration Office of Technology HOUSE BILL No. 1274	"[T]o provide rapid response assistance to a client in need of expert assistance during a cybersecurity incident." House Bill No. 1274 § 5	Advisors and volunteers may be any "individual who has expertise in addressing cybersecurity incidents." Criminal background check and signed contract required. House Bill No. 1274 § 9	Activation/deployment is at the discretion of the State Government Office of Technology.	Immunity from tort or criminal liability. House Bill No. 1274 § 9 Limitations: Must be acting within scope of contract and not engaged in gross negligence or willful/wanton misconduct. House Bill No. 1274 § 9 State Legal Assistance: State "may" provide. House Bill No. 1274 § 9

STATE, AGENCY, LEGAL BASIS	PURPOSE	DEFINITION OF VOLUNTEER	ACTIVATION MECHANISM	INDEMNITY, LIMITATIONS, STATE LEGAL SERVICES
Virginia: Register of volunteer cybersecurity and information technology professionals [NOT PASSED] Under: Virginia Secretary of Administration Proposed Legislation: 2022 H.B. 466	To create “a register of cybersecurity and information technology professionals located across the Commonwealth who are interested in volunteering to assist localities, institutions of higher education, work-based learning programs, and school divisions in addressing information technology and cybersecurity challenges.” Proposed Legislation: 2022 H.B. 466	“[C]ybersecurity and information technology professionals located across the Commonwealth who are interested in volunteering[.]” Proposed Legislation: 2022 H.B. 466	Registered volunteers may take on initiatives to help address cybersecurity and IT challenges in various ways, including mentoring local organizations and schools on best practices in these areas, collaborating with technology education organizations to provide mentorship to students interested in tech and cybersecurity careers, and working with Virginia's regional workforce development offices and the state's Registered Apprenticeship program to create potential pathways for students to get involved in these fields.” Proposed Legislation: 2022 H.B. 466	No statutory indemnification. No state legal assistance provided.

STATE, AGENCY, LEGAL BASIS	PURPOSE	DEFINITION OF VOLUNTEER	ACTIVATION MECHANISM	INDEMNITY, LIMITATIONS, STATE LEGAL SERVICES
STATES WITH PROGRAMS ORGANIZED UNDER STATE AGENCIES				
California: California Cybersecurity Integration Center (Cal-CSIC)/ Cyber Incident Response Team Under: Office of Emergency Services Senate Bill No. 844 (2022 amendments) California Government Code § 8586.5	"[T]o reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in our state. […To] serve as the central organizing hub of state government's cybersecurity activities and coordinate information sharing with local, state, and federal agencies, tribal governments, utilities and other service providers, academic institutions, and nongovernmental organizations." CA Government Code § 8586.5(a)	"The California Cybersecurity Task Force is made up of seven subcommittees each created to address specific Task Force goals. These subcommittees are comprised of volunteers who have families and full-time jobs, but who are passionate about California's cybersecurity." "The California Cybersecurity Task Force consists of representatives from private industry, academia, law enforcement, state government, and California's Federal partners." California Office of Emergency Services Cal-CSIC page	No activation mechanism outside of state direction.	No statutory indemnification. No state legal assistance provided.
Wisconsin: Wisconsin Cyber Response Team (CRT) Under: Wisconsin Emergency Management in coordination with National Guard	"To provide support for critical infrastructure in the state of Wisconsin in order to prevent, mitigate, and respond to cyber incidents through assessments, training, and incident response." Wisconsin Emergency Management CRT page	"Wisconsin's Cyber Response Team has around 200 volunteers, of whom 70 are trained and ready to respond to a cyber incident. CRT members include members of the Wisconsin National Guard and the U.S. Coast Guard, state IT professionals, school and municipal government employees and workers from private organizations." Wisconsin National Guard post on cyber exercise	No activation mechanism outside of state direction.	Acting under direction of state emergency management and National Guard. No apparent legal assistance provided.

STATE, AGENCY, LEGAL BASIS	PURPOSE	DEFINITION OF VOLUNTEER	ACTIVATION MECHANISM	INDEMNITY, LIMITATIONS, STATE LEGAL SERVICES
Oklahoma: Oklahoma Civilian Cyber Corps (OKC3) Under: Oklahoma Cyber Command (National Guard)	"The OKC3 is a team of cybersecurity experts that work to identify, assess, advise on, and assist with responses to cyber events. The goal of the OKC3 is to establish multiple regional teams throughout the state of Oklahoma that can quickly respond to and mitigate the impact of cyber events. These teams will be focused on bolstering cybersecurity defense and response capabilities within Oklahoma communities." Oklahoma Government OKC3 page	To be part of the OKC3 team, individuals must: Be residents of Oklahoma Have at least 2 years of experience in information security, with a preference for those with experience in security operations, incident response, and/or digital or network forensics Pass tests to demonstrate basic knowledge of networking and security concepts Have employer support and sponsorship due to the time commitment required for training and exercises (up to 10 days per year) Pass a background screening Complete a confidential non-disclosure agreement. Oklahoma Government OKC3 page	At direction of Oklahoma Cyber Command.	No apparent indemnification but acting at the direction of Oklahoma state government. No apparent state legal assistance.

STATE, AGENCY, LEGAL BASIS	PURPOSE	DEFINITION OF VOLUNTEER	ACTIVATION MECHANISM	INDEMNITY, LIMITATIONS, STATE LEGAL SERVICES
Maryland: Maryland Defense Force (MDDF) Cyber Security Unit (CYSEC) Under: Maryland National Guard, Maryland Defense Force is "both a volunteer organization and a state agency." Maryland Department of Emergency Management page Created at request of Adjutant General in 2010. 2014 post from MDDF newsletter/blog	"[P]rovides professional, civilian-military expertise in cyber security to the Maryland Military Department and state and local agencies as a service and assistance to their own cyber security programs." MDDF Units Page	Background check, admission to the MDDF, and "2+ years hands-on cyber security experience at a DoD, federal or state agency. DoD 8570 / 8140 Information Assurance Technician certification (CompTIA Security +, CEH, CISSP). An active DoD security Clearance is highly desired. Possession of excellent oral and written communication skills in a professional environment." MDDF Cyber Systems Operator page	At direction of Maryland National Guard and Maryland Defense Force.	Acting at direction of Maryland National Guard, state agency protections may apply.
MULTI-STATE PROGRAM				
Multi-State Information Sharing and Analysis Center Under: Center for Internet Security (nonprofit)	"[T]o improve the overall cybersecurity posture of U.S. State, Local, Tribal, and Territorial (SLTT) government organizations through coordination, collaboration, cooperation, and increased communication." MS-ISAC page	CIS staff voluntarily assist affected members with a variety of cybersecurity needs. "[T]he CIRT, a unit comprised of highly trained and experienced staff, is able to assist you at no cost." MS-ISAC Services Guide	Services provided upon member request. MS-ISAC Services Guide	No statutory indemnification. No state legal assistance provided.
FEDERAL PROGRAMS				
FEMA NET Guard Under: FEMA, now CISA Public Law 107–296, § 224, 6 USC 656: NET Guard	"[T]o assist states and localities in responding to and recovering from incidents that cause significant damage or destruction to IT and communications infrastructure." FEMA, September 16, 2008	"[V]olunteers with information technology (IT) and communications expertise." FEMA, June 18, 2008	"Teams will be a local asset, managed at the local level, and deployed in response to a request from local or State authorities." FEMA, September 16, 2008	No statutory indemnification. No federal legal assistance provision.

STATE, AGENCY, LEGAL BASIS	PURPOSE	DEFINITION OF VOLUNTEER	ACTIVATION MECHANISM	INDEMNITY, LIMITATIONS, STATE LEGAL SERVICES
Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Under: CISA H.R.2471 - Consolidated Appropriations Act, 2022 PUBLIC LAW 117–103 § 101-105. 6 USC 681-681(g) For statutory references in reporting to CISA, see Appendix 4.	"[T]o develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA. These reports will allow CISA to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims." CISA CIRCIA page	Those who voluntarily report information on cyber incidents with CISA. "CISA encourages critical infrastructure owners and operators to voluntarily share with CISA information on cyber incidents." CISA CIRCIA page	On submitting or preparing to submit a report to CISA regarding a cyber incident, protections begin to apply.	Reporting cannot be used in regulatory or enforcement actions against voluntary reporters. 6 USC § 681e(a)(5) Complete liability protections using "No cause of action shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed." Also, no report or preparatory material may be admitted as evidence. 6 USC § 681e(c)(1-3) Limitations: If report is requested by subpoena and not provided, then regulatory actions may be brought under section 681d(c)(2). 6 USC § 681e(c)(1) "[L]iability protections provided in this subsection shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Agency." 6 USC § 681e(c)(2)

Appendix 3
Model Cyber Volunteer Checklist and Agreement for Beneficiaries, Volunteers, Donors and Coordinating Entities

1. Instructions for Model Cyber Volunteer Agreement
2. Checklist of Key Provisions for Model Cyber Volunteer Agreement
3. Template of Model Cyber Volunteer Agreement

    Schedule 1: Statement of Work

    Schedule 2: System and Equipment Access Consent and Authorization

Instructions for Model Cyber Volunteer Agreement

These are instructions to assist with drafting some of the key provisions in the model cyber volunteer agreement that follows. Parties may want to include other details, depending on the type of volunteer activities involved. The below guidance provides background information for some of the provisions.

DISCLAIMER: The information contained in these documents, including these instructions, checklist of key provisions and model cyber volunteer agreement, are for informational purposes only. These documents do not create an attorney-client relationship between McDermott, Will & Emery LLP and you, and are not legal advice. Legal advice must be tailored to the specific circumstances of each case, and the contents of this study are not a substitute for legal counsel. Do not take any action in reliance on the contents of these documents without seeking the advice of counsel.

Parties to the Agreement

Volunteer is the individual that is going to provide assistance with cybersecurity matters.

Beneficiary is the entity that is going to receive the donated cybersecurity volunteer services.

Donor is an entity that is going to donate the volunteer services of its workforce. The name of this party is bracketed throughout the model agreement in case it is not applicable in certain scenarios.

Coordinator is the entity that is responsible for sourcing the volunteer services and facilitating the relationship between the beneficiary and volunteer. The name of this party is bracketed throughout the model agreement in case it is not applicable in certain scenarios.

Equipment

The model agreement provides that a volunteer will use a beneficiary's equipment to provide assistance, but parties may decide whether another party is going to be responsible for the provision of the equipment.

Expense Reimbursement

The model agreement provides options for who is responsible for reimbursing the expenses, if any, that a volunteer incurs in the process of providing volunteer services, but parties may decide whether another party may bear those costs.

Release and Waiver of Liability

The release and waiver of liability provision in the model agreement includes an option for the mutual waiver of claims, but parties or beneficiaries may agree to modify the language and have one party release the other party from claims.

Indemnification

The model agreement provides that a beneficiary will indemnify the parties involved in the provision of volunteer services in case of third-party claims, but parties may decide to eliminate the indemnification provisions altogether.

Recordkeeping

Parties should retain all original, executed cyber volunteer agreements so that they can access the documents when necessary. Consider any retention periods that may be required by law.

Jurisdiction

This model agreement is drafted for US law and does not account for the differences among individual state laws. This model agreement is jurisdiction-neutral. When drafting an agreement, parties should seek legal advice.

If one of the parties is organized or operates in, or any part of the volunteer services takes place in, a foreign jurisdiction, this agreement needs to be modified to comply with applicable laws in the relevant jurisdiction.

Bracketed Items and Modifications

Bracketed items and text in ALL CAPS should be completed with information specific to the particular circumstances. Additionally, in certain circumstances (such as incident response), it may be advisable to modify these agreements to address issues of legal privilege. These agreements have not been drafted with those considerations.

Checklist of Key Provisions for Model Cyber Volunteer Agreement [105]

Description of Provisions to Include

□	Provide a description of the volunteer activities, including a statement of work that will describe the specific tasks with which a beneficiary requires assistance.
□	Describe the nature of the relationship between a volunteer and beneficiary, including disclaiming any employment relationship or benefits, and if applicable, also explain the responsibilities of a donor and a coordinator.
□	Establish criteria for volunteer selection, if any.
□	Require a volunteer to comply with a set of policies and procedures, if any, in the course of providing volunteer services.
□	Set the term or period for the provision of volunteer services and the conditions for terminating the volunteer agreement.
□	Include a beneficiary's consent and authorization permitting a volunteer to access the beneficiary's systems and equipment to perform volunteer services, as required by the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act and the state law equivalents.
□	Determine the responsible party for the provision of necessary equipment and the terms of use of such equipment.
□	Determine the responsible party for reimbursing for possible expenses incurred in the process of performing volunteer services.
□	Require a volunteer, and if applicable, a donor and coordinator, to maintain the confidentiality of a beneficiary's non-public information.
□	Limit access and use of personal data. If volunteer services entail processing of personal data, parties should also consider signing a data processing agreement, if required by law.
□	Include protections for a beneficiary's intellectual property, both pre-existing and created in the course of the provision of volunteer services.
□	Restrict the ability of involved parties to poach volunteers for employment purposes.
□	Restrict a donor's ability to market its own products or services to a beneficiary, if applicable.
□	Include a release and waiver of liability that can be either mutual or one party releasing the other party from third-party claims.
□	Include an indemnification provision that can be either mutual or one party indemnifying the other party, under which parties agree to indemnify the other party for any losses incurred because of the volunteer services.

[105] See Instructions for Model Cyber Volunteer Agreement for important information.

Model Cyber Volunteer Agreement[106]

This Cyber Volunteer Agreement ("Agreement"), dated [___], is entered into [among/between] [___] ("Volunteer"), [___] ("Beneficiary"), [___] ("Donor"), and [___] ("Coordinator"). Volunteer, Beneficiary, [___] ("Donor")], and [___] ("Coordinator") may be referred to as a "Party" and, collectively, as the "Parties."

Background:

A. Volunteer and Beneficiary [Donor, and Coordinator] each desire to enter into the agreement to facilitate the volunteer activities of Volunteer for the benefit of Beneficiary; and

B. Each Party has had opportunity to review this Agreement and obtain or consult with legal counsel of their choice regarding the terms of the Agreement.

Now, therefore, for good and valuable consideration, the sufficiency of which is acknowledged, the Parties agree as follows:

I. Definitions

"**Affiliate**" means all entities that control, are controlled by, or are under common control with Beneficiary and who are thereby bound to the terms of this Agreement.

"**Confidential Information**" means information of Beneficiary that is not publicly available, including but not limited to (i) financial information, (ii) work methods and techniques, relationships, developments, procedures, and concepts, and (iii) Intellectual Property of Beneficiary.

"**Deliverables**" mean any deliverables that Volunteer creates during the performance of specific Services as set forth in the Statement of Work attached hereto as Schedule 1 ("SOW").

"**Intellectual Property**" means all Beneficiary proprietary materials and information, including any technology, software, algorithms, techniques, know-how, and other tangible and intangible items that are owned or developed by or for Beneficiary.

"**Personal Data**" means any information relating to an identified or identifiable natural person.

"**Services**" mean any services set forth in an attached Statement of Work.

"**Statement of Work**" means any description of work attached to this Agreement.

II. Description and Scope of Volunteer Work

[Donor agrees to donate certain members of its workforce and] Volunteer agrees to provide Services to Beneficiary and assist with Services that may include, but are not limited to, preventive actions

[106] See Instructions for Model Cyber Volunteer Agreement for important information.

to improve cybersecurity, incident response or recovery, and cyber vulnerability disclosure programs. The specific Services Volunteer agrees to provide are described in SOW.

III. Relationship among Volunteer [and] Beneficiary[, Donor, and Coordinator]

[Coordinator agrees to source necessary volunteer Services and facilitate the relationship between Volunteer and Beneficiary.] Beneficiary acknowledges that it will receive assistance with Services directly from Volunteer who will demonstrate good faith effort in performing Services, without guaranteeing any outcome. Volunteer [and Donor] acknowledge and agree that Volunteer (i) is not going to be remunerated or compensated for assistance with Services, (ii) is not an employee of [Coordinator or] Beneficiary, and (iii) is not eligible for any employee benefits, such as insurance, health care, worker's compensation, or other benefits. [Donor acknowledges that Volunteer is a member of Donor's workforce and is subject to Donor's organizational policies and procedures, and employee benefit and compensation policies. Donor shall retain exclusive responsibility for all employment matters, including compensation, tax, and social security, insurance, leave, and other employment-related issues.]

IV. Volunteer Selection Criteria and Certification

Volunteer must have [at least one year of] experience working in cybersecurity. Beneficiary, at its sole discretion, may exempt Volunteer from the requirement of minimum work experience. Volunteer certifies that Volunteer is capable of performing the Services and knows of no condition – physical, legal, or otherwise – that would preclude Volunteer's performance of the Services.

V. Compliance with Policies

Volunteer agrees to comply with Beneficiary's [and Coordinator's] organizational policies and procedures, training and safety rules, and conduct expectations.

VI. Term and Termination

This Agreement shall commence on the date indicated above and shall remain in force until terminated by any Party in accordance with this clause. Volunteer's assistance with Services is voluntary, and any Party may terminate this Agreement at any time, for any reason or no reason, provided that they inform, in writing, the other Parties.

VII. Authorization to Access Beneficiary's Systems and Equipment

To perform Services, Beneficiary consents and authorizes Volunteer's access to Beneficiary's systems and equipment pursuant to the authorization in Schedule 2.

VIII. Use of Beneficiary Equipment and Terms of Use

Volunteer will use Beneficiary's IT equipment in accordance with Beneficiary's policies and procedures and only to assist with Services under this Agreement. Any other use of Beneficiary's IT equipment is prohibited.

IX. Expense, Travel, and Reimbursement

Volunteer may perform all work remotely; Parties will discuss and agree on the terms of any travel, if necessary. [Beneficiary / Donor / Coordinator] agrees to reimburse Volunteer for all actual and reasonable expenses, if any, incurred by Volunteer that are attributable to Services performed.

X. Confidentiality

Volunteer[, Donor, and [Coordinator]] agree[s] to protect Confidential Information against unauthorized disclosure. During the term, and after the termination of the Agreement for any reason, Volunteer[, Donor, and [Coordinator]] shall not, directly or indirectly, disclose or communicate to any person or entity or otherwise use any Confidential Information for any purpose, without Beneficiary's prior written approval.

Upon the termination of this Agreement, Volunteer[, Donor, and [Coordinator]] shall promptly return to Beneficiary all documents, records, notebooks, manuals, disks, software, hardware, and other information, as well as all copies thereof, that are Beneficiary's property; provided that a copy of certain materials may be retained as required by applicable law.

XI. Privacy and Data Protection

Volunteer [and Donor] agree to process any Personal Data that Beneficiary makes available in good faith for the specified purposes and on Beneficiary's instructions, and in accordance with applicable laws and regulations. Beneficiary shall limit Volunteer's and [Donor's] access to Personal Data to such Personal Data that is necessary to provide assistance with Services. If the performance of Services requires access to, or sharing of, Personal Data, Parties agree to enter into a Data Processing Agreement covering such processing where legally required.

XII. Intellectual Property

All Intellectual Property, including, but not limited to, copyright and trademarks, related to pre-existing materials that Beneficiary owns and Volunteer uses to perform Services shall remain property of Beneficiary, and no Party shall use for any other purpose other than to provide assistance with Services to Beneficiary. All Intellectual Property rights related to materials that any of the Parties develops in the course of providing assistance with Services, including Deliverables, shall become property of Beneficiary. No Party shall reproduce, copy, or distribute any part of the materials created to perform Services, or disseminate any of its content without prior approval of Beneficiary.

XIII. No Poaching

[Coordinator and] Beneficiary agree not to directly or indirectly employ, offer to employ, or otherwise engage Volunteer during the term of this Agreement without the prior written consent of Donor.

XIV. [No Marketing

Donor acknowledges and agrees that Volunteer's assistance with Services shall not be used as a marketing channel to market, either directly or indirectly, products and services to Beneficiary. Donor is, however, not prevented from engaging in future contractual relationships with Beneficiary, should the Beneficiary request it.]

XV. Release and Waiver of Liability

[Each Party / Beneficiary] hereby releases and discharges other Parties, their Affiliates, subsidiaries, officers, directors, shareholders, employees, agents, representatives, partners, contractors, successors, assigns, and insurers (“Released Parties) from, and expressly waives, all liability, claims, and demands of whatever kind or nature, either in law or in equity, that may arise from Volunteer’s participation in the Services to the full extent permitted by applicable law, with the exception of obligations under the Confidentiality [and Indemnification] provisions. [Each Party / Beneficiary] agrees not to make or bring any such claim or demand against Released Parties, and releases and discharges Released Parties from liability under such claims or demands.

[EACH PARTY / BENEFICIARY] UNDERSTANDS THAT THIS RELEASE DISCHARGES RELEASED PARTIES FROM ANY LIABILITY OR CLAIM THAT [ANY OF THE PARTIES / BENEFICIARY] MAY HAVE AGAINST RELEASED PARTIES ARISING FROM OR RELATED TO SERVICES OR THE RELIANCE BY ANYONE ON SERVICES, THIS DOCUMENT, OR ANY CONTENTS THEREOF.

XVI. Acknowledgment of Risk and Voluntary Participation

Volunteer understands the risks that may arise in a variety of ways associated with Services, and confirms and acknowledges the risks associated with volunteering. With such information and awareness, and with the recognition that other factors may create additional such risks, to the extent allowed by law, Volunteer knowingly, freely, and voluntarily: (a) signs up to volunteer for Beneficiary; (b) engages in volunteer activities; and (c) assumes and accepts the risks of all injury, death, property damage or loss, financial obligation, loss of privacy, loss of reputation, and all other injuries and other consequences, whether known or unknown, whether foreseen or unforeseeable, and whether incurred at Beneficiary facilities or elsewhere, that may result, directly or indirectly, from Volunteer’s presence at Beneficiary facilities or participation as a Beneficiary volunteer, regardless of the cause.

XVII. Indemnification

Beneficiary hereby agrees to indemnify, defend, and hold harmless Volunteer[, [Donor,] and [Coordinator]] from all liability, losses, damages, judgments, or expenses, including attorneys' fees, that it may incur or sustain as a result of negligence, recklessness, or willful misconduct in connection with Volunteer’s participation in the Services, arising out of any third-party claim, including, but not limited to, claims for violations of property trespass, breaking and entering, privacy laws, and computer laws including, but not limited to, 18 USC 1030 and any federal, state, or local laws. Furthermore, Beneficiary shall indemnify and hold Volunteer, [Donor,] and [Coordinator] harmless from any and all liabilities, losses, settlements, judgments, damages, costs, and expenses (including attorneys’ fees), whether as a result of breach of contract, tort (including negligence), or otherwise, regardless of the theory of liability asserted that may arise from or relate to Volunteer’s assistance with Services. Lastly, Beneficiary agrees to come to the aid of Volunteer, [Donor,] and [Coordinator] if local police, sheriff, FBI, FTC, or other governmental or law enforcement agency should detain or question them in any manner during the course of the performance of Services.

XVIII. Governing Law

This Agreement shall be governed by and construed in accordance with the substantive laws of [___], without reference to any choice of law doctrine. Each party [exclusively] submits to the jurisdiction and venue of [____]. [EACH PARTY HERETO IRREVOCABLY WAIVES, TO THE FULL EXTENT PERMITTED BY APPLICABLE LAW, ALL RIGHT TO TRIAL BY JURY IN ANY ACTION, PROCEEDING, OR COUNTERCLAIM ARISING OUT OF OR RELATING TO THIS AGREEMENT OR ANY OF THE TRANSACTIONS CONTEMPLATED HEREBY OR THEREBY.]

XIX. Entire Agreement

This Agreement represents the full understanding among Volunteer, Beneficiary, [Donor,] and [Coordinator] and supersedes all other prior agreements, understandings, representations, and warranties, both written and oral, among the Parties, with respect to the subject matter hereof. If any term or provision of this Agreement shall be held to be invalid by any court of competent jurisdiction, that term or provision shall be deemed modified so as to be valid and enforceable to the full extent permitted. The invalidity of any such term or provision shall not otherwise affect the validity or enforceability of the remaining terms and provisions. This Agreement is binding on and inures to the benefit of Volunteer, Beneficiary, [Donor,] and [Coordinator] and their respective heirs, executors, administrators, legal representatives, successors, and permitted assigns. Section headings are for convenience of reference only and shall not define, modify, expand, or limit any of the terms of this Agreement. This Agreement may be executed in any number of counterparts, each of which is deemed an original, but all of which taken together constitute one single agreement between the Parties.

[Signature Page Follows]

Each of the Parties below has caused this Cyber Volunteer Agreement to be signed and delivered by its duly authorized representative.

[Volunteer]

Signature

Name

Title

Date

[Beneficiary]

Signature

Name

Title

Date

[[Donor]

Signature

Name

Title

Date]

[[Coordinator]

Signature

Name

Title

Date]

Schedule 1[107]
Statement of Work

This Statement of Work ("SOW"), dated [___], describes the volunteer services that [___] ("Volunteer") is going to perform for [___] ("Beneficiary") and is issued pursuant to the Cyber Volunteer Agreement dated on [___] ("Agreement"). Volunteer and Beneficiary may be referred to as a "Party" and, collectively, as the "Parties."

Description of Services

Volunteer will provide Services as directed by Beneficiary to assist with [___].

The Services to be provided may include but are not limited to:

- Task 1: [INSERT THE DESCRIPTION OF THE TASK]
- Task 2: [INSERT THE DESCRIPTION OF THE TASK]
- Task 3: [INSERT THE DESCRIPTION OF THE TASK]

Deliverables

The Deliverables, if any, to be produced in accordance with this SOW are as follows:
[INSERT THE DESCRIPTION OF THE DELIVERABLES]

Term

This SOW will commence on the date specified above and will automatically terminate upon the completion of the last task specified in this SOW, unless extended, in writing, by mutual consent of the Parties.

Exclusions

This SOW is based upon, and is subject to, the following exclusions:

- The Services will start on the date specified above.
- Volunteer is only responsible for the Deliverables described in this SOW. Volunteer shall not be responsible for other parties that Beneficiary may engage during the delivery of the Services unless expressly agreed in writing.
- Volunteer shall not be responsible for delays that Beneficiary or any other party may cause.
- The Services hereunder are non-transferable.

Terms and Conditions

Volunteer Services shall be subject to the Agreement, which shall be incorporated by reference into this SOW. In case of any material conflict between the terms in the Agreement and the terms in this SOW, the terms in the Agreement shall control. Any terms not defined herein shall have the meanings defined in the Agreement.

[107] See Instructions for Model Cyber Volunteer Agreement for important information.

Schedule 2
System and Equipment Access Consent and Authorization[108]

Beneficiary has engaged Volunteer to provide assistance with Services specified in the applicable SOW. Beneficiary confirms that it has consented and authorized Volunteer to receive access to its systems and equipment necessary for Services ("Authorization").

In consideration of Volunteer's access to Beneficiary's systems and equipment, Volunteer understands and agrees as follows:

1. To perform the Services, Volunteer may, among other things, [DESCRIBE THE TYPE OF ACCESS REQUIRED TO PERFORM SERVICES].

2. Beneficiary acknowledges that, despite precautions that Volunteer takes to avoid damage to Beneficiary's network and systems, disruptions, outages, and/or data loss may occur as a result of performing Services.

3. Beneficiary understands that all systems on its network or otherwise accessible during Services should be backed up prior to the provision of Services.

4. Beneficiary will provide to Volunteer certain information required for performing Services, such as a description of the systems and networks. Beneficiary represents and warrants that to the best of its knowledge, all information provided is true and accurate and that as between the Parties, Beneficiary owns or leases or is authorized to represent the owners of the systems, networks, facilities, and/or devices described in connection with Services.

5. Beneficiary may notify all or some of its employees, contractors, and other third parties about Services that Volunteer is going to perform.

6. No day and time restrictions apply to the Services.

7. Beneficiary will allocate appropriate working space and physical access for Volunteer if Volunteer needs to perform Services on-site at Beneficiary's premises.

8. Beneficiary will make available key stakeholders that can best help plan action items for Services.

[108] See Instructions for Model Cyber Volunteer Agreement for important information.

Appendix 4
Legal Issues in Vulnerability Disclosure and Bug Bounty Programs

There are three main forms of legal protections related to reporting cybersecurity vulnerabilities: legal protections attached to vulnerability reporting requirements by federal law, vulnerability disclosure programs (VDPs), and bug bounty programs.

Indemnifications for Reporting to CISA

Unauthorized cyber volunteers have some measure of legal indemnification if they report vulnerabilities to CISA under both a 2015 and a recent 2022 statute. The Cybersecurity Information Sharing Act of 2015[109] specifies that information shared pursuant to the act retains applicable privileges, including trade secret protection, and makes explicit that these protections adhere "notwithstanding any other law."[110] These protections apply fairly broadly within the area of cyber threat indicators and defensive measures, though to be eligible for the act's protections, the information must be sanitized of personally identifiable information and shared with the federal government through specifically authorized mechanisms.[111]

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) offers immunities related to entities who report a cyber vulnerability to CISA from both regulatory action and any legal action, both directly and by protecting the materials used in preparing such reports from being used as evidence.[112] These entities could be organizations that have suffered a cyber incident, but the protections apply to anyone who files such a report and therefore could be extended to anyone who reports their vulnerabilities and findings to CISA through CIRCIA's accepted methods.[113]

VDPs

VDPs are a way of capturing unauthorized and altruistic cybersecurity activities.[114] In 2020, CISA issued Binding Operational Directive 20-01[115] requiring all federal agencies to develop a VDP. The directive distinguished such

[109] Cybersecurity Information Sharing Act of 2015, § 105(d)(1). Available at: (https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%202015.pdf).

[110] *Id.,* Sections 104(a)-(c). This broad language overrides existing federal surveillance, privacy, and antitrust law as well as state laws.

[111] *Id.,* see Section 102(6) for broad types of information covered as threat indicators and Section 104(d)(1) for information on the security controls necessary.

[112] Information shared with or provided to the Federal Government, 6 U.S. Code § 681e((c)(1-3)).

> "No cause of action shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed for the submission of a report pursuant to section 2242(a) that is submitted in conformance with this subtitle and the rule promulgated under section […] The liability protections provided in this subsection shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Agency"
>
> […] "[N]o report submitted to the Agency pursuant to this part or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, provided that nothing in this part shall create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting such report."

[113] Cyber Incident Reporting for Critical Infrastructure Act of 2022 (https://www.cisa.gov/circia) (last visited Jan. 22, 2023).

[114] *See* A Framework for a Vulnerability Disclosure Program for Online Systems, Department of Justice (July 2017) (https://www.justice.gov/criminal-ccips/page/file/983996/download) (last visited Jan 25. 2023).

[115] Binding Operational Directive 20-01 – Develop and Publish a Vulnerability Disclosure Policy (https://www.cisa.gov/binding-operational-directive-20-01) (last visited Jan. 22, 2023).

programs from bug bounty programs (which are not required) and stating "[a] vulnerability disclosure policy []is an essential element of an effective enterprise vulnerability management program and critical to the security of internet-accessible federal information systems." CISA's directive requires a commitment "not to recommend or pursue legal action" against those who engage with the VDP in "good faith," which is defined as "accessing a computer or software solely for purpose of testing or investigating a security flaw or vulnerability and disclosing those findings in alignment with the VDP" and which is often determined by a "factual, timely report of a vulnerability on a system authorized for testing, sent directly to the organization in accordance with a VDP's instructions."[116]

Bug Bounty Programs

Bug bounty programs, in contrast, offer a form of legal indemnification and (often) financial support for otherwise unauthorized computer security testing. However, bug bounties are usually run by the corporations most at risk from vulnerabilities, such as Microsoft[117] and Intel[118], and offer limited legal protections for those engaged in relevant activities, with extensive caveats. For example, Microsoft's bug bounty program has extensive terms and conditions,[119] but those who qualify and follow appropriate procedures benefit from the Microsoft Bounty Legal Safe Harbor, which states that Microsoft considers "security research and vulnerability disclosure activities conducted consistent with this policy to be 'authorized' conduct under the Computer Fraud and Abuse Act, the DMCA, and other applicable computer use laws such as WA Criminal Code 9A.90."[120] Microsoft also states that it reserves "the sole right to make the determination of whether a violation of this policy is accidental or in good faith, and proactive contact to us before engaging in any action is a significant factor in that decision. If in doubt, ask us first!"[121]

Still, bug hunting has received the imprimatur of the US Department of Defense (DOD) through its Hack the Pentagon initiative and through DARPA's Finding Exploits to Thwart Tampering (FETT) Bug Bounty, under which bug bounties are offered to individuals affiliated with private-sector Silicon Valley firms that engage in bug hunting by crowdsourcing digital defense.[122][123] In 2018, the DOD offered a contract to three firms to coordinate their affiliated security professionals and incentivize them through bug bounties: Synack,[124] HackerOne[125] and Bugcrowd.[126]

[116] *Id.* at subheading: What does the directive mean by "good faith"? (https://www.cisa.gov/binding-operational-directive-20-01#what-does-the-directive-mean-by-good-faith).

[117] Microsoft Bug Bounty Program (https://www.microsoft.com/en-us/msrc/bounty) (last visited Jan. 22, 2023).

[118] Intel: Bug bounty program (https://www.intel.com/content/www/us/en/security-center/bug-bounty-program.html) (last visited Jan. 22, 2023).

[119] Microsoft Bounty Terms and Conditions (https://www.microsoft.com/en-us/msrc/bounty-terms?rtc=1) (last visited Jan. 22, 2023).

[120] Microsoft Bounty Legal Safe Harbor (https://www.microsoft.com/en-us/msrc/bounty-safe-harbor) (Jan. 22, 2023).

[121] *Id.*

[122] DARPA Announces First Bug Bounty Program to Hack SSITH Hardware Defenses (2020) (https://www.darpa.mil/news-events/2020-06-08a).

[123] Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital Defense Program (2018) (https://www.defense.gov/News/Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/).

[124] Synack (https://www.synack.com/company/) (last visited Jan. 22, 2023).

[125] HackerOne (https://www.hackerone.com/) (last visited Jan. 22, 2023).

[126] Bugcrowd (https://www.bugcrowd.com/) (last visited Jan. 22, 2023).

Appendix 5
Bibliography

(ISC)² 2021. "A Resilient Cybersecurity Profession." *isc2.org.* 2021. https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

21st Century Infrastructure Commission. *21st Century Infrastructure Commission Report.* Nov 30, 2016. https://www.michigan.gov/documents/snyder/21st_Century_Infrastructure_Commission_Report_555079_7.pdf.

Beougher, Stephanie. "Ohio Cyber Reserve member deployed in cybersecurity response." *The Ohio Adjutant General's Department.* Feb 18, 2021. https://ong.ohio.gov/stories/2021/feb/20210218-ocr-deployment.html.

—. "Ohio Cyber Reserve members train to assist with cybersecurity issues." *The Ohio Adjutant General's Department.* Nov 9, 2021. https://ong.ohio.gov/stories/2021/nov/20211129-ohcr-training.html.

Brooks, Sean. *Digital Safety Technical Assistance at Scale.* June 2020. https://cltc.berkeley.edu/wp-content/uploads/2020/06/Digital_Safety_Technical_Assistance_at_Scale.pdf.

Center for Digital Resilience. *Center for Digital Resilience Value Pillars.* Dec 19, 2022. https://digiresilience.org/about/#pillars.

CISA. "BINDING OPERATIONAL DIRECTIVE 20-01 - DEVELOP AND PUBLISH A VULNERABILITY DISCLOSURE POLICY." *CISA.gov.* Sept 2, 2020. https://www.cisa.gov/binding-operational-directive-20-01.

CiviCERT. *Computer Incident Response Center for Civil Society.* Dec 19, 2022. https://www.civicert.org/.

Cohen, Natasha, and Peter Warren Singer. "The Need for C3: A Proposal for a United States Cybersecurity Civilian Corps." *NewAmerica.org.* Oct 25, 2018. https://www.newamerica.org/cybersecurity-initiative/reports/need-c3/.

Consortium of Cybersecurity Clinics. Dec 19, 2022. https://cybersecurityclinics.org/.

Cruickshank, Jennifer, and Iain J. Cruickshank. "We Need A Cybersecurity Awareness Campaign And Civil Defense Force." *TaskAndPurpose.com.* July 10, 2018. https://taskandpurpose.com/news/we-need-a-cybersecurity-awareness-campaign-and-civil-defense-force/.

Cyber Safety Review Board. "Review of the December 2021 Log4j Event." *CISA.gov.* July 11, 2022. https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf.

CyberPeace Institute. Dec 19, 2022. https://cyberpeaceinstitute.org/cyberpeace-builders.

Cyberspace Solarium Commission. "March 2020 CSC Report." *Cybersolarium.org.* Mar 11, 2020. https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report/ (accessed February 6, 2023).

Dr. Goolsby, Rebecca. "On Cybersecurity, Crowdsourcing, and Social Cyber-Attack." *Wilson Center.* 2013.

https://www.wilsoncenter.org/sites/default/files/media/documents/publication/127219170-On-Cybersecurity-Crowdsourcing-Cyber-Attack-Commons-Lab-Policy-Memo-Series-Vol-1.pdf.

Dr. Smith, Maggie. "Taking the Elf Off the Shelf: Why the U.S. Should Consider a Civilian Cyber Defense." *LawFare.* July 6, 2022. https://www.lawfareblog.com/taking-elf-shelf-why-us-should-consider-civilian-cyber-defense.

FEMA. "FEMA Announces Awards to Pilot Citizen Corps National Emergency Technology Guard (Net Guard) Program." *FEMA.gov.* Sept 16, 2008. https://web.archive.org/web/20080918062718/http://www.fema.gov/news/newsrelease.fema?id=45806.

—. "FEMA Announces Solicitation to Pilot Citizen Corps National Emergency Technology Guard (Net Guard) Program." *FEMA.gov.* June 18, 2008. https://web.archive.org/web/20080716094419/http://www.fema.gov/news/newsrelease.fema?id=43909.

Greater Geneva Bern Area. "Geneva welcomes the CyberPeace Institute." *ggba-switzerland.ch.* Oct 2, 2019. https://www.ggba-switzerland.ch/geneva-welcomes-the-cyberpeace-institute/.

Hansen, Liane, and Sen. Ron Wyden. "NETGuard: High-Tech Volunteers to the Rescue?" *npr.org.* June 29, 2008. https://www.npr.org/templates/story/story.php?storyId=92008366.

Hatmaker, Taylor. "Synack is the latest cybersecurity company to offer state elections its services for free.″ June 6, 2018. https://techcrunch.com/2018/06/06/synack-election-security-states/.

Herras, Ray, Jack Janson, Takayuki Miyazaki, Marie Natsvlishvili, Shenhav Ruttner, and Yushan Xu. "Helping Cities Respond When A Cyber-Attack Strikes: Leveraging Cyber and Technology Professionals as Volunteers During a Response." *Columbia School of International and Public Affairs.* May 2020. https://www.sipa.columbia.edu/academics/capstone-projects/helping-cities-respond-when-cyber-attack-strikes.

Kallberg, Jan. "Demilitarize civilian cyber defense, and you'll gain deterrence." *DefenseNews.* Feb 9, 2022. https://www.defensenews.com/opinion/commentary/2022/02/09/demilitarize-civilian-cyber-defense-and-youll-gain-deterrence/.

Kapelke, Chuck. "Cybersecurity Clinics Create Online Defense for the Public Good." *newamerica.org.* July 5, 2022. https://www.newamerica.org/the-thread/cybersecurity-clinics-create-online-defense-for-the-public-good/ (accessed Jan 9, 2023).

Kerner, Sean Michael. "US Department of Defense Expands Bug Bounty Efforts." *eweek.com.* Oct 24, 2018. https://www.eweek.com/security/us-department-of-defense-expands-bug-bounty-efforts/ (accessed January 9, 2023).

Lachow, Irving. "Equity and Diversity in the Nation's Cyber Workforce: Policy Recommendations for Addressing Data Gaps." *Center for Strategic & International Studies.* Apr 2022. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220405_Lachow_Cyber_Equity.pdf?0bZKVinRnTdtukT4P0uVKNDAbuGoQvPc.

Michigan Department of Technology, Management & Budget. "Michigan Cyber Civilian Corps (MiC3)." *michigan.gov.* Dec 19, 2022. https://www.michigan.gov/dtmb/services/cybersecurity/michigan-cyber-civilian-corps-mic3.

—. "Michigan Cyber Civilian Corps (MiC3)." Oct 18, 2022. https://www.michigan.gov/dtmb/services/cybersecurity/michigan-cyber-civilian-corps-mic3.

Michigan Senate. "Cyber Civilian Corps Act. Act 132 of 2017." *Michigan Legislature.* Jan 24, 2018. https://www.legislature.mi.gov/documents/mcl/pdf/mcl-Act-132-of-2017.pdf.

Nash, Kim S. "Tech and Manufacturing Firms Launch Industrial Cybersecurity Group." June 7, 2022. https://www.wsj.com/articles/tech-and-manufacturing-firms-launch-industrial-cybersecurity-group-11654596000.

National Governors Association. "Re-Envisioning State Cyber Response Capabilities: The Role Of Volunteers In Strengthening Our Systems." *nga.org.* June 16, 2022. https://www.nga.org/publications/re-envisioning-state-cyber-response-capabilities-the-role-of-volunteers-in-strengthening-our-systems/.

National Institute of Standards and Technology (NIST). "Framework for Improving Critical Infrastructure Cybersecurity." *National Institute of Standards and Technology.*[repetitive of first item in this entry? *NIST.gov* as in entry below?] Apr 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

—. "Glossary, Small Business Cybersecurity Corner." *NIST.gov.* Feb 28, 2019. https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary.

Ohio Adjutant General's Department. *Ohio Cyber Reserve (OhCR). ong.ohio.gov.* Oct 18, 2022. https://www.ong.ohio.gov/special-units/cyber/ohcr/index.html.

—. "Ohio Gov. Mike DeWine signs cyber reserve legislation. News release." *ong.ohio.gov.* Oct 25, 2019. https://ong.ohio.gov/press-releases/2019/20191025-log29.pdf.

—. *OHIO CYBER COLLABORATION COMMITTEE (OC3).* Oct 18, 2022. https://www.oc3.ohio.gov/.

Ohio Senate. "S.B. No. 52, 133rd General Assembly, Regular Session 2019-2020." *General Assembly of the State of Ohio.* Oct 11, 2021. https://search-prod.lis.state.oh.us/solarapi/v1/general_assembly_133/bills/sb52/IN/00?format=pdf.

Pattison-Gordon, Jule. "What Makes a State Volunteer Cybersecurity Program Work?" June 14, 2021. https://www.govtech.com/security/what-makes-a-state-volunteer-cybersecurity-program-work.

National Governors Association. "Re-Envisioning State Cyber Response Capabilities: The Role Of Volunteers In Strengthening Our Systems." *nga.org.* June 16, 2022. https://www.nga.org/center/publications/re-envisioning-state-cyber-response-capabilities-the-role-of-volunteers-in-strengthening-our-systems/.

Romaniuk, Scott, and Mary Makjikian. *Routledge Companion to Global Cyber-Security Strategy.* London and New York: Routledge, 2020.

Ruiz, Monica M. "Is Estonia's Approach to Cyber Defense Feasible in the United States?" Jan 9, 2018. https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/.

—. "Is Estonia's Approach to Cyber Defense Feasible in the United States?" *warontherocks.com.* Jan 9, 2018. https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/[This appears to be a duplicate of the prior entry].

Seffers, George I. "Calling for a Civilian Cyber Corps: Experts tout the benefits of an army of civilian hackers." *Signal*. May 2019: 41-43.

Smith, Gerry. "The Nerd Reserves: Sandy Recovery Renews Call For Tech National Guard." *huffpost.com.* Nov 23, 2012. https://www.huffpost.com/entry/tech-national-guard_n_2168374.

State of Wisconsin Division of Enterprise Technology. *Cyber Response Team Program (CRT)[Page title is "Response Teams" and the setion referenced is titled "Wisconsin Cyber Response Team (CRT)"].* Oct 18, 2022. https://wem.wi.gov/response-teams/#ctr.

Sterling, Bruce. "Estonian Cyber Security." *wired.com.* Jan 9, 2018. https://www.wired.com/beyond-the-beyond/2018/01/estonian-cyber-security/.

Sullivan, Stephen, and Diana Garza. "Supply Chain Risks, Cybersecurity and C-TPAT, a Literature Review." *Research Association for Interdisciplinary Studies.* Aug 16, 2021. https://ideas.repec.org/p/smo/lpaper/0082.html.

Temple-Raston, Dina, and Will Jarvis. "'A nerd's gotta do what a nerd's gotta do:' Why Craig Newmark is funding a cyber civil defense." Apr 20, 2022. https://therecord.media/a-nerds-gotta-do-what-a-nerds-gotta-do-why-craig-newmark-is-funding-a-cyber-civil-defense/.

Texas State Legislature. "SB 475." *texas.gov.* June 14, 2021. https://capitol.texas.gov/BillLookup/History.aspx?LegSess=87R&Bill=SB475.

U.S. House of Representatives. "Public Law 107-296 – Homeland Security Act of 2002." *DHS.gov.* Nov 25, 2002. https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf.

U.S. Senate – Homeland Security and Governmental Affairs. 117th Congress (2021-2023). *S.1324 – Civilian Cybersecurity Reserve Act.*[Remove italics and add quotation marks to match leglislation cited immediately above?] Apr 22, 2021. https://www.congress.gov/bill/117th-congress/senate-bill/1324.

U.S. Senate Committee on Armed Services. "FULL COMMITTEE HEARING: U.S. Strategic Command and U.S. Cyber Command." *armed-services.senate.gov.* Mar 12, 2013. https://www.armed-services.senate.gov/hearings/oversight-us-strategic-command-and-us-cyber-command.

This material is for general information purposes only and should not be construed as legal advice or any other advice on any specific facts or circumstances. No one should act or refrain from acting based upon any information herein without seeking professional legal advice. McDermott Will & Emery* (McDermott) makes no warranties, representations, or claims of any kind concerning the content herein. McDermott and the contributing presenters or authors expressly disclaim all liability to any person in respect of the consequences of anything done or not done in reliance upon the use of contents included herein. *For a complete list of McDermott entities visit mwe.com/legalnotices.

McDermott
Will & Emery

mwe.com