Zombies, Sirens, and Lady Gaga – Oh My!
Developing a Framework for Coordinated Vulnerability Disclosure for U.S. Emergency Alert Systems

Amy Woszczynski [a], Andrew Green [b*], Kelly Dodson [c], Peter Easton [d]

[a] Department of Information Systems, Kennesaw State University, 560 Parliament Garden Way NW, MD 0405, Kennesaw, GA 30144-5591, USA.
[b] Department of Information Systems, Kennesaw State University, 560 Parliament Garden Way NW, MD 0405, Kennesaw, GA 30144-5591, USA. awoszczy@kennesaw.edu
[c] Department of Information Systems, Kennesaw State University, 560 Parliament Garden Way NW, MD 0405, Kennesaw, GA 30144-5591, USA
[d] Department of Information Systems, Kennesaw State University, 560 Parliament Garden Way NW, MD 0405, Kennesaw, GA 30144-5591, USA
[*] Corresponding author: (678) 390-0038, agreen57@kennesaw.edu

Declarations of interest: none

Abstract

U.S. emergency alert systems (EAS) run on legacy software with aging hardware and limited cybersecurity. While EASs are an essential component of the U.S. critical infrastructure, they are often under-funded, and workers frequently lack the knowledge to protect these systems adequately. Recent compromises of various EASs have not inspired public confidence. We present a method for EAS authorities to engage with external cybersecurity researchers to find, recover from, and disclose vulnerabilities using coordinated vulnerability disclosure (CVD) policies. Clearly written CVD policies set guidelines and legal bounds for cybersecurity research, taking advantage of researcher expertise while working to strengthen the cybersecurity of the patchwork public-private-government networks comprising EASs. We intended to investigate the CVD policies of EASs in seven southeastern states; however, we could find no CVD policies through the entire supply chain. Instead, we investigated the CVD policies of the top 10 technology firms on the Fortune 500 list, analyzing best practices in terms of publication of a CVD policy, as well as: setting eligibility requirements, describing the submission process, delineating researcher restrictions, outlining agreements on sharing credit, and explaining bounties (if relevant). We recommend that EAS authorities develop CVD policies in line with suggested criteria, using policies from top technology organizations combined with the proposed framework, and using cybersecurity researchers as a valuable component of the EAS supply chain.

Keywords:

government, policy, emergency alert system, critical infrastructure, coordinated vulnerability disclosure, cybersecurity researcher, cybersecurity policy

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

1. Introduction

Emergency alert systems (EASs) are part of the critical infrastructure of the United States, serving as a method of informing affected groups of developing weather conditions, wildfires, hazardous materials, nuclear bombs, and other disasters at the national, state, local, or regional level. Federal law requires EASs to: "implement the public alert and warning system to disseminate timely and effective warnings regarding natural disasters, acts of terrorism, and other man-made disasters or threats to public safety" (6 U.S. Code § 321o. Integrated public alert and warning system modernization (2), 2016). The EAS itself, however, is vulnerable to attacks on its widely dispersed network of public, private, and government partners. When EASs distribute inaccurate information, the public notices. For instance, EAS distributed a Lady Gaga video instead of an Emergency Alert Notification (EAN) in 2011 (Clayton, 2011); warned of the zombie apocalypse in 2013 (Ollmann, 2013; Roberts, 2013; Reuters, 2013; Storm, 2013); turned on the sirens in the middle of the night for over an hour in Dallas in 2017 (Dixon, 2018; Hub, 2017), and alerted Hawaiians of an incoming ballistic missile in 2018 (Kang, 2018). In each of these cases, adversaries took advantage of cybersecurity policy failures, including: the use of unchanged default passwords; a failure to follow proper operating procedures when updating systems; the transmission of insecure radio waves; and many other system vulnerabilities. While we cannot prevent a zombie apocalypse or some real emergency, EAS authorities have the power to develop and implement policies to reduce the vulnerability of the system itself and decrease the likelihood of access by unauthorized individuals, organizations, or bots. This increases confidence in the alerts sent to the population as a whole. Zombie apocalypse announcements, blaring sirens when there is no emergency, ballistic alert notices sent by mistake, and Lady Gaga

videos, in contrast, reduce the perceived validity of EAS announcements and may cause people to disregard the messages as inaccurate, unimportant, or misleading.

Internal security policies provide one method of protecting the integrity of messages sent by EAS authorities, although breaches have resulted from the failure to properly implement and enforce these policies (Ayyagari, 2012). A well-staffed cybersecurity team, which implements and updates policy measures, develops training for employees, and monitors the system for disruptions, is essential to protect EASs. Most EASs, like other critical infrastructures, suffer from inadequate cybersecurity funding for ongoing maintenance (Brem, 2015; Goff, 2017; Norris, Joshi, & Finin, 2015; Sales, 2013; Wolff & Lehr, 2018), hampering their ability to protect their systems, and non-compliance with cybersecurity training programs (Norris et al., 2015). In fact, Sales (2013) notes that funding for cybersecurity in critical infrastructure is "missing the mark by a wide margin." Without adequate funding, partners in the network struggle to continuously test, update, and protect the technology components that comprise the EAS; we propose that cybersecurity researchers, if used properly, may help to ease the funding shortfall.

Cybersecurity researchers, sometimes derogatorily called "hackers" (Eichensehr, 2017), have a problematic relationship with organizations they study. On the one hand, the researchers identify vulnerabilities as part of their everyday activities. The identification of unknown vulnerabilities may benefit the organization, depending on the course of action it takes once discovered. Does the cybersecurity researcher privately disclose the vulnerability to the organization first, and then disclose to the public in a coordinated manner, allowing the organization to protect the vulnerable system from those who would do it harm? Alternatively, does the cybersecurity researcher decide to share the information publicly, immediately upon discovery of the

vulnerable system? More importantly, does the organization have an effective method for the researcher to disclose the vulnerability while protecting from legal prosecution? If so, is the statement clearly displayed and publicly available?

In a perfect world, after finding a vulnerability, the cybersecurity researcher would notify the organization, the organization would resolve the vulnerability and make a public announcement after resolution, crediting the researcher who reported the problem. However, the real world is not that simple. From the perspective of the cybersecurity researcher who identifies the problem, concern over potential civil or criminal penalties makes it difficult to determine how or if to disclose vulnerable systems, particularly when trying to understand inconsistent, often confusing, federal, local, and state laws (Kosseff, 2018). Moreover, since only 6% of Forbes Global 2000 companies had any sort of responsible disclosure policy in 2015 (Branscombe, 2017), cybersecurity researchers may be legitimately confused about how to inform the organization and receive credit for discovering the vulnerability. Further, current legislation at the federal and state levels discourages cybersecurity research activities and reduces the likelihood that researchers will report a newly discovered vulnerability (Kosseff, 2018) even with Matwyshyn (2017) calling for: "intervening before an attack occurs, not merely after" and creating a legal set of "formalized feedback loops engaging technical experts." Coordinated vulnerability disclosure (CVD) policies, which allows cybersecurity researchers to report vulnerabilities without fear of legal penalties, is one step toward pre-attack intervention.

This paper analyzes how cybersecurity researchers, private and public organizations, and governmental agencies can work together to develop and implement CVD policies. We begin with an overview of the U.S. EAS before turning to cybersecurity researchers and disclosure of vulnerabilities. Then we collect CVD policies from top firms on the Fortune 500. We conclude

with guidelines for cybersecurity researchers and organizations to harmoniously work together to identify and resolve vulnerable systems in EASs.

2. Background

2.1 Review of Emergency Alert Systems

2.1.1 History

In 1934, the Federal Communications Commission (FCC) specifically assigned control of radio and wire communication in the event of a national emergency to the U.S. President; 47 U.S. Code Section 606 granted these powers, which states that: "…the President is authorized, if he finds it necessary for the national defense and security, to direct that such communications as in his judgment may be essential to the national defense and security shall have preference or priority with any carrier" (47 U.S. Code § 606 - War Powers of President). The day after the attack on Pearl Harbor, Roosevelt addressed the Congress and declared war on Japan. While radio networks covered Roosevelt's speech, CBS News, as one of the early providers in the new television industry, broadcast the first widely distributed emergency warning, when it reported on the attack at Pearl Harbor; although Sunday was a non-programming day, the station interrupted its scheduled day off, and began covering the news of the attack (Conway, 2006). There has been tension, however, between military and Presidential control of communications, particularly during times of peace and in the lead-up to a war (Winkler, 2016).

The first system broadcast to notify residents of an emergency weather situation occurred in 1947, followed by the introduction of Control of Electronic Radiation (CONELRAD) by the Truman administration in 1951, to alert citizens in the case of a nuclear attack during the Cold War (Brinson, 2009). CONELRAD was never intended to notify local populations of adverse weather events and is beyond the scope of this paper. In 1951, President Truman signed the Federal Civil Defense Act into law (United States Congress, 1950). This legislation authorized

the creation of the Federal Civil Defense Agency and tasked it with, among other responsibilities, the provisioning of a communications system to spread warnings of enemy attacks (Cohen & Boyer, 1951).

The current network of U.S. EASs, the focus of this paper, has evolved to reach as much of the affected population as possible; while EASs began with notification of the population via radio, they then moved to television, and recently added mobile and wireless capabilities (McFarlane, 2017). EASs were established to use "broadcasters, cable television systems, wireless cable systems, satellite digital audio radio service providers, direct broadcast satellite service providers and wireline video service providers" (Federal Communications Commission (FCC), 2018) during a national, state, or local emergency, and to include AMBER Alerts and emergency weather information.

As a part of the nation's critical infrastructure, we should minimize erroneous messages on the interconnected EASs, with significant safeguards in place to ensure the system is secured and protected from threats. Thus, when the affected populations receive an alert, they can be confident that the information is valid, reliable, relevant, timely, and real-world. If there are too many inaccurate alerts, the public will likely question the information provided, even during an actual emergency. However, incorrect announcements, errors, and security breaches have been around since the network's inception. In 1971, an emergency alert submitted throughout the EAS network warned that global nuclear war was about to occur (Diaz, 2012); fortunately, many broadcast stations thought it was a test and did not send the announcement, and authorities issued a correction shortly after the alert.

In the 1990s and 2000s, entities began to distribute information on a wide-scale over the Internet. By 1997, the current EAS, which includes television, radio, cable, satellite, and wireless, evolved

from the originally established Emergency Broadcast System (Emergency notification system definitive guide, n.d.), which focused on television (and radio) alerts. Internet access became ubiquitous, and curious people began to look for vulnerable systems, or they happened upon the systems by chance. With the addition of wireless and mobile devices, EAS authorities hoped that global positioning system (GPS) technology would allow quick and easy distribution of alerts to the affected population, based on their location. However, current GPS technology has proven less effective than expected (Kang, 2018), and authorities continue to look for ways to distribute the messages to all people in an affected area, without alarming others outside the bounds of the emergency.

Errors became noticeable to this widely dispersed and Internet-connected population. For instance, in 2007, a contractor inadvertently left a satellite distribution receiver on, and Illinois state officials accidentally sent an Emergency Action Notification (EAN), a direct message from the President of the United States (FEMA Fact Sheet, 2007), a system which has never been used for a real-world national emergency; after the incident, FEMA promised increased coordination throughout the interconnected EAS network. Coordinating among and between different entities in the supply chain is difficult. We concur with FEMA's recommendation and suggest that the EAS supply chain seek mutually beneficial and clearly communicated vulnerability disclosure policies that benefit the public, the entities involved with EASs, and cybersecurity researchers, who identify and disclose vulnerable systems.

2.1.2 Vulnerable systems in the EAS network

It is well-known that EASs are vulnerable to access by unauthorized users (Constantin, 2013). State and local governments are under constant security attacks (Norris et al., 2015); since many of the partners on the EAS network are agencies of the state and local government, we contend that EAS networks similarly face an ongoing attack of vulnerable systems. Thus, protecting

EASs is a matter of public safety; EASs must provide reliable, accurate, updated, and timely information to the population at risk. U.S. law (Emergency Management 6 U.S. Code § 321o. - Integrated public alert and warning system modernization (b)(5)) states that emergency management authorities must, "to the extent practicable, ensure that the public alert and warning system is resilient and secure and can withstand acts of terrorism and other external attacks." However, there are no specific guidelines on how to make the system resilient and secure, how much funding to invest in secure systems, or how to test the information security of the network. Sometimes, vulnerable systems emerge due to limited access to cybersecurity professionals, throughout the EAS network (Hub, 2017). Since the systems run on interconnected networks of public-private-governmental partnerships and through numerous local, state, city, county, and federal jurisdictions, it is reasonable to assume that some links throughout the network may have cybersecurity challenges; thus, all links in the network risk attack through the least secure point (McGuire, 2018). Add the problems of decreased funding for security initiatives (Hub, 2017; McFarlane, 2017), difficulty recruiting top cybersecurity talent with expertise in emergency management (Walker, 2012), and inconsistent cybersecurity policies implemented throughout the supply chain (Miron & Muita, 2014), and securing vulnerable systems becomes a daunting task; an overarching plan to secure EASs is difficult, time-consuming, and complicated. Further, working with numerous partners in the EAS supply chain and different vendors makes cybersecurity for critical infrastructure an even more difficult task (Morrison, 2013). When considering only basic cybersecurity maintenance for existing U.S. national critical infrastructure assets, a staggering cost of about $3.6 billion is needed (Hemme, 2015). In the last ten years, according to Forbes, the U.S. government spent $100 billion on cybersecurity and was predicted

to spend at least $14-28 billion in 2016 (Mason, 2018; Morgan, 2015). Clearly, the amount of spending on cybersecurity is a non-trivial matter.

With the reality of limited funding for national critical infrastructure assets, EAS authorities may need to find alternative ways to secure digital assets, identify vulnerabilities when they occur, and reward cybersecurity researchers who find and report vulnerabilities in line with coordinated disclosure policies. EAS authorities should welcome a low-cost, high-quality knowledge base of cybersecurity researchers into this complicated system. While cybersecurity researchers provide a "free" check of system vulnerability, the EAS network does not make it easy for them to report their findings. Most links in the EAS network do not identify and publish policies to encourage the disclosure of vulnerabilities in a coordinated manner.

Vulnerable systems are a reality for the interconnected EAS system in the U.S. To protect EASs, it is crucial to understand potential adversaries. If public, private, and government links in the EAS supply chain start with the assumption that systems are only vulnerable to highly skilled computer science experts, they lose the cybersecurity game before the players take the field. Cybercriminals with limited knowledge of the system can gain administrative system access and exploit the vulnerable system (Dodril, 2016). EAS authorities should consider the development of policies that encourage reporting of vulnerable systems while working together with public, private, and government partners to develop CVD policies. Thus, cybersecurity researchers become part of the EAS team and increase the chances of reducing vulnerabilities or identifying vulnerabilities when they occur.

2.1.3 Public-private-government partnerships

Although many authors have championed the use of public-private-government partnerships to improve the security of critical infrastructures, such as EASs (Borchert, 2015; Claus, Gandhi, Rawnsley, & Crowe, 2015; Eichensehr, 2017; Manley, 2015; Marett, 2015), there has been little

practical implementation or testing of such partnerships. In this complex network, sharing of information with partners in the chain is needed to maintain the efficiency of the overall network (Karlsson, Kolkowska, & Prenkert, 2016). However, this valuable ability to share with those in the EAS supply chain comes at the cost of potentially vulnerable systems in the interconnected system (Meshkati & Tabibzadeh, 2016); this is particularly true in the EAS network, where most nodes on the network are privately owned and operated (Borchert, 2015; Claus, Gandhi, Rawnsley, & Crowe, 2015; Egli, 2013), with an insular focus on individual success. (Eichensehr, 2017) argued that government and public/private organizations, which should be partners, function more as individual entities, operating in their own best interests to the detriment of the group's best interests, with widely varying cybersecurity policies throughout the network. Frequently patches are issued too slowly for critical infrastructure, and organizations have to establish a backup plan to minimize risk to their vulnerable systems (Wirth, 2017), especially when they are dealing with critical infrastructure systems.

Systems development should consider integrating cybersecurity initiatives at all levels and throughout the entire EAS supply chain. However, while EAS authorities develop their systems and networks with expert technical knowledge, a creative, synergistic approach may be more useful to design, plan, and implement appropriate levels of risk management and cybersecurity into EASs. Direct involvement of stakeholders with local knowledge allows the implementation of community-centric networks, which can be designed to reach people in the methods that will be most effective (Baudoin, Henly-Shepard, Fernando, Sitati, & Zommers, 2016). Moreover, instead of relying solely on an in-house cybersecurity team, EAS authorities could rely on networks of cybersecurity researchers and other entities in the EAS supply chain, to help improve the cybersecurity of vulnerable systems.

Much like fusion centers that link law enforcement with public and private agencies to streamline and secure the services they offer (Carter, Carter, Chermak, & McGarrell, 2017), EASs use a distributed network of security partners. Despite cybersecurity challenges, the EAS must be able to connect securely and quickly across multiple partners in the supply chain, particularly in large-scale disasters that span multiple cities, counties, localities, states, and even countries. To cybercriminals, the weakest link in the EAS may offer a jumping-off point to others in the highly interconnected network. For instance, Lockheed Martin suffered a cyberattack in 2011, and the cybercriminals may have been able to compromise other military contractors who shared information, including potentially damaging information on weapons and military design (Rodin, 2015). Similarly, cybercriminals compromised Target's network to access customer credit card information by using the credentials of an HVAC subcontractor (Krebs, 2014). While Lockheed and Target are not EAS networks, they are part of an extensive, fragmented network, and they illustrate potential problems when associating with partners who do not use appropriate levels of security to protect data and information.

The public-private-government partnerships established for much of the U.S. critical infrastructure qualify as an inter-organizational system whose cybersecurity policies should be regularly evaluated. Borchert (2015) asserts that organizational security and national security are intertwined. As cloud computing and other distributed systems continue to proliferate, it is incumbent upon governmental agencies at the federal, state, and local levels to seek partnerships with companies who view cybersecurity as a strategic priority. Recognizing the interconnected relationship of these networks and the importance of protecting critical infrastructure at all levels, some authors (Claus, Gandhi, Rawnsley, & Crowe, 2015) suggested training National Guard units as cyber warriors to respond to local security crises or partnering with universities to

simulate and overcome threats to vulnerable systems. Another example of synergistic partnerships to protect critical infrastructure was the U.S. Army's "Hacking for Defense" program, which put together a partnership between students, academics, practitioners, cybersecurity researchers, and troops in developing secure systems to solve defense-related problems (Crown, 2017). States have recognized opportunities for improving cybersecurity through partnerships, such as in Michigan, where authorities established the Cyber Civilian Corps to be activated if needed during a State of Emergency (Michigan, 2018), and in Arkansas, where Army and Air Force National Guard troops are being trained on cyber threats and are ready to assist if needed during an attack on critical infrastructure (Condit, 2018). Other states are considering similar opportunities to use National Guard troops for cybersecurity initiatives related to critical infrastructure systems.

EASs receive government funds to operate; however, government funds are variable and may change from year to year. Links in the EAS supply chain may need to consider other methods of integrating cybersecurity into the systems they maintain. With numerous cybersecurity researchers who are already testing systems and identifying vulnerabilities, perhaps they could provide a method of improving cybersecurity at low or reduced costs. We look at cybersecurity researchers in more detail in the next section.

2.2 Cybersecurity researchers

2.2.1 What is a cybersecurity researcher?

We begin by operationalizing what cybersecurity researchers do and how they may help federal, state, or local EASs. Eichensehr (2017) equates security researchers to hackers, and says that they find vulnerabilities and attack them, and then send the methods of attack to others. However, all cybersecurity researchers are not hackers, although the two groups may share similar motivations of money, reputation, information exchange or current or future job

opportunities (Hausken, 2017; Laszka, Zhao, Malbari, & Grossklags, 2018). While the negative view of cybersecurity researchers is pervasive, other authors have recognized the value of collaboration with security experts, with McNeil (2018) encouraging complex networks to embrace these "cybersecurity ninjas" and use their expertise to improve the networks. Cybersecurity researchers are as diverse as information technology professionals, specializing in different areas of expertise while knowing a little bit about many potential vulnerabilities. An overarching characteristic of the cybersecurity researcher is the need to follow a code of ethics (Takanen, Vuorijärvi, Laakso, & Röning, 2004). Adherence to codes of ethics will vary, depending on the background, expertise, and training of the researcher. Cybersecurity researchers may be employed in public or private organizations, by the government, work as freelance technology reporters or function as individual researchers with a curious nature and desire to serve society. They may investigate malware, track adversaries based on previous patterns, and/or build profiles of attackers for future identification, using automated tools and previous experience to find vulnerable systems; further, they frequently check security and vulnerability forums and social media to learn about new, developing, ongoing, and resolved information security issues (Yasin, 2016). Cybersecurity researchers are typically knowledgeable in computer forensics, computer programming and ethical security research behaviors, according to the FBI, who hires cyber special agents to: "conduct multifaceted investigations of high-tech crimes, including cyber-based terrorism, computer intrusions, online exploitation and major cyber fraud schemes" (Yerak, 2015). Similarly, the U.S. Army hires Information Technology Program Managers (Policy and Planning Information Security), who "lead the design, development, assignment, and governance (to include system and application security design, evaluation, and policy)" for the LandWarNet projects; further, the U.S. Army applicant must be a

problem solver and a good communicator, among other qualifications (USAJobs, 2018). Cybersecurity researchers investigate different issues each day and must perform work that is not routine; they solve problems that other people do not even realize exist.

Estimating the number of cybersecurity researchers is difficult. With over 100,000 jobs predicted for "information security analysts" in 2017 by the Bureau of Labor Statistics (Occupational Employment Statistics, 2017), and continued growth and unfilled positions, we can assume that they number in the hundreds of thousands, if not more. The next section describes the diverse background and preparation undertaken by cybersecurity professionals.

2.2.2 Preparing cybersecurity professionals

The U.S. government, recognizing their substantial need for cybersecurity professionals, offers several programs to help develop the field. Academics may apply to the "Hacking for Defense" or "Hacking for Diplomacy" programs through Cyber Command; these programs allow students to work on a real-world problem identified by the professor or the students, if approved (What is Hacking for Defense, n.d.). Interestingly, almost half of the students working on these real-world projects ultimately accept a cyber-related government position upon graduation. These partnerships and outreach activities are developing a qualified pool of candidates for cybersecurity positions that are difficult to fill. Colleges such as Carnegie-Mellon and University of Tulsa (Nakashima & Soltani, 2014) specifically teach offensive skills to cybersecurity researchers, although they note the importance of strong ethical foundations in their programs. They contend that students need exposure to offensive skills so they can protect critical infrastructure. Researchers, cybersecurity professionals, government officials, and educators have not yet reached a consensus, however, on whether students should study defensive capabilities in isolation, or whether in combination with offensive capabilities, when preparing cybersecurity professionals for real-world opportunities.

2.2.3 Understanding cybersecurity disclosure policies

Ideally, cybersecurity researchers should read and evaluate a company's disclosure policy before doing any research on potentially vulnerable systems (Laszka, Zhao, Malbari, & Grossklags, 2018). However, since most cybersecurity researchers find vulnerabilities by accident (Kranenbarg, Holt, & van der Ham, 2018), requiring them to ask permission or read the rules before they find a vulnerability is impractical. Understanding what behaviors are allowed, as well as those that are not, may save cybersecurity researchers from potential civil and criminal liability. The trend in the U.S. is toward punishment of cybersecurity researchers. Typically, when a cybersecurity researcher finds a vulnerable system, officials often spend significant time and effort attempting to find and prosecute the researchers who identified and reported the security problem (McFarlane, 2017). Rather than punishing these researchers, organizations may benefit by utilizing the information and working with cybersecurity researchers to repair the vulnerability, while also alerting those who might be affected. Interacting with the cybersecurity researchers may be particularly beneficial for scarce information regarding vulnerable systems; that is, high value and potentially significant impact information (Matwyshyn, Hacking speech: Informational speech and the First Amendment, 2013). Attrition (2016) agrees, suggesting that organizations should embrace cybersecurity researchers and improve cybersecurity through continuous refinement of systems and prompt response to those who report vulnerabilities. Even development of secure IT systems has moved to an ongoing process of improvement over time (Wrona, et al., 2018), and in this environment, cybersecurity researchers may be able to contribute to the process and reduce the vulnerability of critical infrastructures such as the EAS.

2.2.4 Negative perceptions of cybersecurity researchers

While some may view cybersecurity researchers negatively, they may be able to provide valuable assistance to bolster the cybersecurity of critical infrastructure systems like the EAS. A clear way of distinguishing between hackers and cybersecurity researchers might improve societal perceptions and make partnerships between security researchers and EAS authorities more likely. EAS links in the supply chain may be able to coordinate with cybersecurity researcher groups, who espouse democracy and individual privacy rights. The Chaos Computer Club in Europe, for instance, has sought to protect individual privacy (Kubitschko, 2015). If they – and similar organizations – are encouraged to expand their work and protect the personal safety of individuals by improving critical infrastructures such as EASs, there is no reason to expect that they would not respond. The problem is how to solicit them and encourage them to participate in security activities to improve systems without causing damage. Clear, front-facing, easily accessible CVD policies could help as described in the next section.

2.3 Coordinated Vulnerability Disclosure (CVD)

Legal limitations make it difficult for cybersecurity researchers to evaluate vulnerabilities if they are afraid of being arrested or sued in a civil case. Complicating matters even further, the government may classify many types of information on national security grounds, raising concerns about freedom of speech, accountability, and freedom of information (Nasu, 2015). The development of clear, unambiguous policies is beneficial to all levels of the EAS supply chain. McNeil (2018) specifically recommends "the development of a comprehensive coordinated vulnerability disclosure program" and that "proper procedure and efforts are consistently applied to the repair of all vulnerabilities and prevention of future damages." Jump (2019) suggests collaborating with cybersecurity researchers as part of a "formal coordinated vulnerability disclosure process," while Suárez & Scott (2017) suggest that, "a coordinated vulnerability

disclosure process is a critical component of a well-rounded product security program." McNeil, Jump, and Suárez & Scott are referring to the security of biomedical devices; however, the distributed nature of the EAS, with public-private-governmental partnerships, and the need for top levels of security, compares well to the shared critical infrastructures comprising the EAS.

2.3.1 Responsible disclosure vs coordinated disclosure

Partners in the EAS network should consider treating cybersecurity researchers in the private sector and those in academia, as mutual partners in securing critical infrastructures. As valued stakeholders, EAS authorities could encourage cybersecurity researchers to disclose discovered vulnerabilities in a proficient manner, with no fear of criminal or civil penalties for their work. Many argue for the implementation of responsible vulnerability disclosure, or similarly named alternatives. A responsible vulnerability disclosure policy "…addresses how a vulnerability identifier should disclose vulnerability information to appropriate people, at appropriate times, and through appropriate channels in order to minimize the [public] loss associated with vulnerabilities" (Cavusoglu, Cavusoglu, & Raghunathan, 2007). A modified version of responsible disclosure is known as coordinated vulnerability disclosure (CVD) (Schuster et al., 2017). While responsible disclosure refers to the good faith effort on behalf of the researcher who is disclosing, CVD refers to the close relationship between the organization and the researcher, with mutually beneficial outcomes (Kranenberg, Holt, & van, 2018). The organization acquires another professional to identify vulnerabilities, and the researcher receives recognition, future job opportunities, compensation, or intrinsic rewards from helping others. With CVD, the key is cooperation between information asset owners and those who discover vulnerabilities, find solutions, and reduce risks (ISO/IEC 29147, 2014). Further, CVD allows EAS authorities to control legal risks through self-regulation, specifying how they want people who are in and around their systems to behave. Unlike other disclosure mechanisms, CVD

motivates the vendor to release a patch to resolve a vulnerability (Cavusoglu, Cavusoglu, & Raghunathan, 2007) and equally motivates the cybersecurity researcher to be a good partner and steward of the vulnerability knowledge by adhering to the agreed-upon CVD policy. In fact, Matshwhyn (2017) suggested that organizations who do not patch known vulnerabilities should be banned from the network. With CVD, authorities often give public credit or other incentives (such as bug bounties) to the researcher or researchers. Disclosing in a coordinated manner helps to "balance the need for freedom and privacy by providing enough time to correct issues while still keeping the public informed" (Bonderud, 2014); this is a mutually beneficial activity that comes at little cost to the researcher or the organization.

2.3.2 Development of policies

EAS authorities would be well-served through the development of clearly written CVD policies, which will have a two-fold benefit: 1) they allow organizations to tap into a talented group of highly motivated and cybersecurity researchers; and 2) they provide a way for cybersecurity researchers to contribute to strengthening EASs without being concerned about legal repercussions. However, for this mutually beneficial situation to work, EAS authorities must have clearly written CVD policies, and the cybersecurity researcher must follow them precisely. However, even in The Netherlands, one of the few countries with a national vulnerability disclosure process, security researchers still fear legal penalties for reporting vulnerabilities (Kranenbarg, Holt, & van der Ham, 2018). Authorities should not penalize those who disclose cybersecurity breaches when being evaluated for future government contracts, as long as the breach has been resolved (Rodin, 2015). If the government penalizes cybersecurity researchers by not awarding future contracts, it is reasonable to speculate that fewer breaches will be made public. Rather than penalizing those who announce breaches, the federal government should reward them, since higher performing organizations voluntarily report cybersecurity breaches in

annual reports (Li, 2015) on their websites, and in applications for future government contracts. Cooperative forward-looking policies on cybersecurity would be more likely to prevent cyberattacks than punishment of organization after a vulnerability has been exploited (Kosseff, 2018; Sales, 2013).

2.3.3 Legal considerations

Before disclosing a vulnerability, cybersecurity researchers have to consider risks, rewards, and potential outcomes or penalties associated with the potential disclosure. Marett (2015) calls this a manipulation check. As long as the effort (reward) exceeds the cost (punishment), cybersecurity researchers will continue investigating vulnerabilities; the same goes for reporting vulnerabilities. To protect themselves, cybersecurity researchers should ensure that scanning is accurate and authorized by the organization (Dittmer & Wright, n.d.). Even if the intent is criminal, the risks of getting caught, prosecuted, and ultimately jailed for investigating vulnerabilities are low, with easy access to useful applications and tools to scan for and penetrate vulnerable systems (Metivier, 2017). To protect themselves, EAS authorities need to approach the system like a cybersecurity researcher looking for vulnerabilities and like a hacker hoping to exploit vulnerabilities.

To date, there is little consensus on how the patchwork of federal, state, and local laws applies to cybersecurity researchers. For instance, David Level and Scott Moulton faced both civil and criminal penalties based on state laws, in Florida and Georgia respectively, when they found a vulnerability that they were not authorized to investigate. In Florida, David Level exploited systems allowing plaintext access to Florida's elections website. After Level attacked the system, he disclosed the vulnerabilities online and was later arrested for felony theft (Osborne, 2016). Alternatively, consider Scott Moulton in Georgia, who conducted an unauthorized test of a 911 system that was part of a Cherokee County police department network, which would

connect to his client, the City of Canton (Network Installation v. VC3, 2000). Moulton contended he had an ethical obligation to ensure the cybersecurity of any systems linked to the City of Canton. Of note, while Level exploited the vulnerable system he identified and then disclosed online, Moulton did not profit from, damage, or publicly disclose the vulnerabilities he discovered. Both Level and Moulton found vulnerable systems; however, neither had authorization to look for the vulnerabilities in the first place, and both faced repercussions, rather than rewards, for finding and exploiting the vulnerable systems. These cases have different situational contexts; however, they demonstrate a more significant problem of complex state laws that lead ethical security researchers to be cautious when finding and reporting vulnerabilities.

Combine confusing and often conflicting state laws with federal laws, such as the Computer Fraud and Abuse Act (CFAA), which includes several portions that alarm cybersecurity researchers (Calabrese, 2017; Matwyshyn, 2017; Peterson, 2015), and the situation becomes even more complicated. For instance, when AT&T accidentally published iPad user information on their website, Andrew Auernheimer and Daniel Spitler found the vulnerability, wrote a script to send themselves the names as proof of the vulnerability, and then reported the vulnerability to Gawker (Zetter, 2016). After being convicted of violating the CFAA and receiving a prison sentence, Auernheimer's attorneys appealed the decision, arguing that accessing a public website cannot be a violation under the act (Fakhoury, 2014). While the appeals court granted the appeal due to an incorrect trial venue, the ruling was silent on the issue of whether federal prosecutors could use the CFAA to criminally charge cybersecurity researchers for simply visiting an open public website. Other cases abound where authorities used the CFAA to penalize those who do cybersecurity research. Facing serious legal or civil consequences for disclosing vulnerabilities,

cybersecurity researchers often find little reason to report vulnerable systems they discover. Matwyshyn (2017) suggests revising the CFAA to clearly outline how cybersecurity researchers may legally identify and report vulnerabilities, which would open the door for a more coordinated approach to vulnerability discovery, disclosure, and remediation to educate members of the EAS network.

The potential for civil and criminal penalties beyond the CFAA, at the state, local, city, county, and municipality levels, likely deters disclosure even more. If laws criminalize cybersecurity research activities, it is a two-fold blow. Researchers cannot analyze and study technology trends, protection techniques, malware, and vulnerabilities, for fear of being prosecuted. Moreover, if they do find vulnerable systems, they may stay silent about them for fear of being prosecuted by the government on criminal charges, or sued by the organization in civil court. In addition, cybersecurity researchers may flock to jurisdictions receptive to their activities, whether at the federal, state, or local levels, or even outside of the U.S. States face the possibility of losing top cybersecurity researchers to other states, and the U.S. may lose these highly trained cybersecurity researchers to other nations which understand the value of those who disclose. Alternatively, EASs authorities may lose the opportunity to identify and resolve vulnerable systems before an invalid ballistic missile alert is sent, for instance, with a cascading loss of public credibility associated with incorrect announcements.

While cybersecurity researchers often argue for First Amendment protection for their speech, the courts have not yet reached a consensus on whether research reports on vulnerable systems qualify for Constitutional protection. Matwyshyn (2013) proposes a 4-prong test for determining if a cybersecurity researcher's speech is protected, including the speaker's intent, where the researcher reports their findings, the scarcity of the information, and the reasonable risks of

adverse outcomes as a result of disclosure. However, current legislative efforts often ignore the intent of the researcher, instead criminalizing many routine cybersecurity researcher activities – no matter the intent. Complicating matters further, federal law may provide additional penalties for information security researchers, even where state law is more lenient. To better understand the myriad legal challenges faced by cybersecurity researchers, we examined existing laws on accessing computer systems without authorization in seven southeastern states: Alabama, Florida, Georgia, North Carolina, South Carolina, Tennessee, and Virginia. We chose the southeastern U.S. since the area is well-positioned for technology projects (Sangster, 2008) with projected growth in the sector. We also chose the region because of the diverse laws passed by the states, including recent legislative updates and proposed changes in laws that have generated national interest. This sample provides a reasonable starting point for our research, although we concede that results may be limited, no matter what sections of the U.S. we study. As a first analysis of CVDs for EASs within a region of the U.S., the research provides a starting point from which to build an additional understanding of EASs across the country and across the world.

We found that state laws differ, as shown in Table 1. Most of the southeastern states we evaluated included harmful intent as a qualifier, particularly when assessing the violation as a misdemeanor or felony. For example, Florida and North Carolina evaluate the willing and knowing access of state computer networks based on harmful intent, such as disruption of services, extortion, or cyber-bullying (FL Code § 815-06, 2019; N.C. Gen. Stat. § 14-453 to 14-458). Similarly, Alabama's Computer Crime Act and Tennessee law evaluate the harm that results when a user "intentionally and without authorization" accesses state computer networks; if no harm results, the violation is a misdemeanor, while if sufficient harm results, the violation

may be a felony (AL Code § 13A-8-13; TN Code § 39-14-602, 2018). Virginia's Computer Crimes Act (VA Code § 18.2-152.1 to 152.15) only makes access of computer systems illegal if harm results; however, the law does state that "A person is guilty of the crime of personal trespass by computer when he uses a computer or computer network to cause physical injury to an individual." Thus, scanning for vulnerabilities is not covered directly, although it may be considered a form of illegal personal trespass by computer. South Carolina has the most stringent laws when it comes to information security researchers, making it illegal to use scanners to access computer systems without authorization (S.C. Code § 16-16-10 to 16-16-40). In effect, South Carolina does not allow cybersecurity researchers to scan systems for vulnerabilities, regardless of intent. While Georgia follows most of the other southeastern states in requiring knowledge and harmful intent (OCGA § 16-9-93), in 2018, Georgia Senate Bill 315, which removed the harmful intent requirement, passed through the state legislature. Cybersecurity researchers and high-profile technology firms like Google and Microsoft criticized the bill and asked Governor Deal to veto it (Green, 2018). The bill, which also would have allowed offensive measures as retaliation (sometimes called "hacking back" or "back hacking") for unauthorized access, was vetoed by Gov. Nathan Deal after the negative feedback he received (Gallagher, 2018). Even in the rare case where state laws do not criminalize investigating system vulnerabilities, federal legislation may deter cybersecurity researchers. For instance, DefCon participants reported concerns that federal laws, such as the Digital Millennium Copyright Act, may constrain legitimate cybersecurity research (Lynch, 2016). Thus, the cybersecurity researcher is left to determine lawfulness based on a confusing set of state and federal guidelines.

Table 1. Southeastern States and Laws Regarding Disclosure of Vulnerabilities

State	Relevant Laws	Highlights

Alabama	AL Code § 13A-8-13	Provides greater penalties for harmful intent
Florida computer authority; not is often	FL Code § 815-06-01	Makes it illegal to access another's system, knowingly and without whether one intends to do harm or not relevant.
Georgia	Ga. Code §§ 16-9-90 to 16-9-94, §§ 16-9-150 to 16-9-157	Must have harmful intent to be prosecuted[1]
North Carolina	N.C. Gen. Stat. § 14-453 to 14-458	Makes it illegal to access another's computer system, knowingly and without authority; whether one intends to do harm or not is often not relevant.
South Carolina	S.C. Code § 16-16-10 to 16-16-40	Makes it illegal to access another's computer system, without authority; also makes it illegal to use scanners to access computer systems without authorization.
Tennessee	Tenn. Code Ann. § 39-14-601	Makes it illegal to access another's computer system, knowingly and without authority; whether one intends to do harm or not is often not relevant.
Virginia	Va. Code § 18.2-152.1 to 152.15	Must have harmful intent to be prosecuted

Once the cybersecurity researchers navigate the complex laws at the federal and state levels in the U.S. and find a vulnerability, they must decide what to do with the information they possess. The risk of legal consequences increases when cybersecurity researchers report vulnerabilities,

[1] Senate Bill 315, which created a new crime of "unauthorized access" and increased penalties, was passed by the Georgia Assembly. Gov. Nathan Deal vetoed Senate Bill 315 on May 8, 2018 (http://www.legis.ga.gov/Legislation/en-US/display/20172018/SB/315

especially those found without the consent of the system's owner (Matwyshyn, 2013). As some state laws criminalize even unintentional access and legitimate cybersecurity research, it may become more difficult to find qualified people, particularly for governmental jobs that already struggle to match industry salary (Nixon, 2016; Yasin, 2016); in fact, the number of unfilled cybersecurity jobs is expected to reach 3.5 million in 2021 (Mason, 2018). With a fragmented system of patchwork laws across the U.S., cybersecurity researchers are continuously dealing with legal uncertainties (Peeters, 2017). Since a wide variety of state and federal laws consider all forms of hacking – and "hacking" is rarely clearly defined – as a criminal offense, uncertainty and risk to cybersecurity researchers continues unabated, discouraging rather than encouraging cooperative efforts (Kosseff, 2018). Cybercriminals with malicious intent can brazenly attack systems, while cybersecurity researchers must consider legal consequences when deciding if they report vulnerabilities, encountered through legitimate cybersecurity research. Even as Karlsson et al. (2016) and others call for researchers to test the security of highly connected systems, possible legal penalties loom. By not having CVD policies in place, EAS authorities are shutting out cybersecurity researchers who may want to help resolve the threats to vulnerable systems. Many cybersecurity researchers will disclose at no cost, while some may prefer a bug bounty if they find a vulnerable system or a simple acknowledgment for identifying and reporting the vulnerable system. With current legislation, testing of inter-organizational security by cybersecurity researchers, including testing of critical infrastructure such as EASs, is very limited. Alternatively, if cybersecurity researchers do find vulnerable systems, they may not share it with those who need to know, for fear of reprisal. A clearly worded, publicly available, and highly promoted CVD process may improve the chances of receiving feedback from cybersecurity researchers, although few organizations have such a policy (Branscombe, 2017).

Complicating reporting of vulnerabilities, it is sometimes hard to determine the owner of a particular portion of the highly interconnected EAS network. Without knowing the owner, the cybersecurity researcher does not know who should receive the vulnerability report. EAS authorities, in turn, do not have the bandwidth to secure the systems they manage, and they lack the expertise, funding, and guidance needed to develop and implement CVD policies. Further, there are not enough qualified applicants for available cybersecurity positions (Morgan, 2015). This paper seeks to link EAS authorities with the large pool of underutilized cybersecurity researchers throughout the world. However, it is unrealistic to believe that these researchers will work for free. There are many methods of incentivizing cybersecurity researchers, as described in the next section.

2.3.4 Rewarding cybersecurity researchers

It is difficult to prove that cooperative, responsible disclosure leads to better results than other policies or no policy at all. Diverse groups of cybersecurity researchers gather information on vulnerabilities every day. Their information security expertise may be free, or perhaps based on rewards from a bug bounty program. With high prices for the disclosure of zero-day vulnerabilities, there have to be incentives for the cybersecurity researcher to disclose in a responsible manner (Eichensehr, 2017). There are several touted examples of using CVD successfully, particularly when paired with a reward. Capitalizing on the skills of cybersecurity researchers, both the Mozilla Foundation and Google implemented a successful bug bounty program for their respective Firefox and Chrome web browsers; with tiered reward systems, fast response times, and gamification (through competitions) of the identification of vulnerabilities, both companies have reported successful outcomes with good returns on investment (Finifter, Akhawe, & Wagner, 2013). Using crowdsourcing for security vulnerability testing has proven effective in other organizations, especially if the researchers are incentivized to find and report

security issues (McFarlane, 2017). Domdouzis, Akhgar, Andrews, Gibson, & Hirsch (2016) report that crowdsourcing models have worked to prevent crime after an emergency; we speculate that such a model might work well for testing and maintaining highly interconnected EASs as well. The Department of Defense, which is a highly distributed network of federal, local, and state networks, used crowdsourcing in its first bug bounty program, “Hack the Pentagon," encouraging cybersecurity researchers to find and disclose vulnerabilities in the public-facing portions of some Department of Defense sites (DoD News, 2016). In that program, the federal government partnered with HackerOne (Hack the Pentagon, n.d.), offering an undisclosed dollar amount for reporting vulnerabilities, provided that the researcher followed the disclosure guidelines established (DoD Vulnerability Disclosure Policy, 2016). This straightforward disclosure policy may serve as a starting point for other local, state, and federal critical infrastructure systems, like the EAS. Asking for help from the untapped potential of cybersecurity researchers offers significant opportunities to strengthen critical infrastructure. "Hack the Pentagon” is the first time that the federal government offered a bounty to cybersecurity researchers (DoD News, 2016). Because of its success, the Department of Defense launched “Hack the Army” (Signal, n.d.) and “Hack the Air Force” (Seals, 2017) bug bounty programs as well. By capitalizing on the highly-skilled, highly-motivated cybersecurity researchers, and seeking partnerships with them, rather than serving as antagonists, the EAS network may be well-positioned to adopt Matwyshn’s (2017) recommendations to anticipate and predict vulnerabilities before they occur, while embracing a shift in thinking and legal priorities. Particularly as adversaries become more numerous and better trained (Wrona, et al., 2018), the use of cybersecurity researchers outside of the traditional public-private-government partnerships increases the opportunity to find and mitigate new threats as they emerge.

Establishing a reward (or bounty) for those who disclose vulnerable systems in a coordinated manner is akin to the suggestion to incentivize those who would invest in infrastructure improvements (Egli, 2013). Cybersecurity researchers in public and private organizations, as well as in government positions and academia – or simply others who are interested in and possess knowledge about security vulnerabilities – are identifying vulnerabilities that EAS authorities often do not have the time, funding, or expertise to find. Liaisons could coordinate with cybersecurity researchers and establish CVD policies to strengthen the public-private-government partnership and improve critical EAS infrastructure. A clearly specified CVD policy could protect cybersecurity researchers from fear of legal reprisals as they complete legitimate research. While the potential penalties for reporting vulnerabilities are high, the penalty for not reporting is nothing; not reporting frees the researcher from potential penalties and leaves the organization with unidentified vulnerabilities (Kranenberg, Holt, & van, 2018), a lose-lose situation. However, before cybersecurity researchers can be embraced by the coalition of public, private, and government EAS stakeholders, the generally negative perceptions of these potential partners have to be overcome.

2.3.5 Recommendations

When designing CVD policies, experts make several recommendations. The website should include a dedicated email for reporting vulnerabilities and a method of communicating with the researcher throughout the process (Branscombe, 2017), keeping them informed and engaged. While Cavusoglu et al. (2007) describe social loss as a component of CVDs, we modify slightly for the EAS in particular, and refer to it as a public loss, or the total loss caused by a vulnerable EAS, including developing a resolution for the identified vulnerable system and the costs incurred throughout the EAS supply chain due to damage, data leakage, penalties, loss of confidence, perceived lack of ability to manage crises, and potential injury or loss of life to the

constituencies served. Public loss potential is high, and EAS authorities should establish CVD policies to minimize risks.

While there are several forms of vulnerability disclosure, almost all vulnerability analyses and research activities are illegal under current laws (Peeters, 2017). Further, most government agencies do not share data, so if cybersecurity researchers run vulnerability scans or test systems, they might very well go to jail (Karlsson, Kolkowska, & Prenkert, 2016) or at the least, be sued in civil court. We contend that EAS authorities are overlooking one of their greatest resources – cybersecurity researchers. If EAS authorities fail to implement CVD policies which encourage research, testing, and disclosure, the outlook for our critical infrastructure is bleak. Current funding levels do not offer the resources needed to identify and resolve all the vulnerabilities within the EAS network of providers.

CVD policies should provide mutual benefits to EAS authorities and cybersecurity researchers who identify the vulnerability. With a stated CVD policy, the EAS, the researcher, and the public are all protected. Cybersecurity researchers understand that a CVD process will ensure that the owners in the EAS supply chain will act to overcome the vulnerability. The researcher needs to have options, however, if the organization decides not to implement a fix, or if they delay the patch indefinitely; in that case, the cybersecurity researcher may choose to release the data to the public to force the developer to find a way to overcome the problem (Davis, 2015). Sometimes the researcher who finds the vulnerability sets a time limit for the development of a patch (Bonderud, 2014); in that way, cybersecurity researchers ensure that the organization has access to timely information and develops a plan to resolve the vulnerability.

CVD policies ensure personal recognition for the discoverer of the vulnerability. If, however, there is no CVD process, the cybersecurity researcher may disclose immediately. The best option

for both sides is to reach a coordinated agreement on reporting and resolving vulnerabilities while retaining flexibility if one side or the other does not meet their respective portions of the agreement.

2.4 Vulnerability Reporting and Handling

Cybersecurity itself, and CVD policies specifically, are still young in terms of testing implementations, and there is not yet an agreed-upon standard for disclosure (Lynch, 2016). Thus, we sought guidance from reputable industry standards: The International Organization for Standardization (ISO) and National Institute of Standards (NIST). ISO/IEC 29147 (2014) is relevant to the discussion, since it deals with how to handle and resolve the sub-area of vulnerability disclosure. While ISO/IEC 30111 (2013) is also of interest when identifying vulnerabilities, it deals more specifically with internal disclosures and is beyond the scope of this paper. NIST (2018) deals more generally with cybersecurity, recommending five core cybersecurity functions: identify, protect, detect, respond, and recover. We combine elements of ISO and NIST, along with the limited academic research available, to create a framework for CVD that follows a step-by-step process to create, implement, monitor, and resolve vulnerabilities.

No matter the reward given or the categories of eligible disclosers or the types of disclosures allowed, EAS authorities should consider establishment of a CVD process using industry standards. A robust cybersecurity governance mechanism coupled with a CVD policy is likely to lead to more resilient EASs; they will be more secure and more effective, wisely using the cybersecurity researchers who are available at little to no cost. Moreover, while the medical device field has adopted some ISO components with modest success (Lechner, 2017), the adoption of ISO standards has not been widespread (Coalition, 2016). Clearly communicated CVD policies are a step in the right direction, as long as the members of the EAS supply chain

describe specific guidelines on disclosure, which protect the researchers and the members of the public-private-government EAS network.

2.5 Guidelines for Developing Coordinated Vulnerability Disclosure Policies

While we hoped to evaluate components of published CVDs of EAS providers in the Southeast, we could not locate such guidelines. Thus, we sought guidance from established industry frameworks, ISO and NIST, along with the work of Laszka, Zhao, Malbari, & Grossklags (2018) and others, to develop a simplified framework that EAS authorities may use for developing CVD policies. The ISO framework has been embraced by industry, although government agencies may be slow to adopt. In fact, Matshwyn (2017) specifically recommends issuance of an executive order that requires all government organizations, which would include partners in the EAS network, to follow ISO guidelines. In the sections that follow, we describe a framework, developed through a combination of industry and academic guidelines, with five key foundations of CVD: eligibility, submission and verification, restrictions, credit, and bounty.

2.5.1 Eligibility

Eligibility identifies who may be considered for rewards or public recognition, for disclosing vulnerabilities. Laszka et al. (2018) refer to this component as in-scope and out-of-scope areas, while HackerOne (2017) uses the term scope. ISO/IEC 29147 (2014) outlines how the organization must stand ready to receive and respond to vulnerability disclosures reported by cybersecurity researchers, ensuring that eligible reporters are clearly delineated. With NIST (2018), setting eligibility components is in line with identifying the vulnerability – from whom and in what manner system vulnerabilities may be reported.

2.5.2 Submission and verification

Once an eligible cybersecurity researcher finds a vulnerability, they need to know how to submit the report to the EAS, and what the organization will do after next. Setting submission requirements is in line with ISO/IEC 29147 (2014), which requires that organizations are ready

to respond to reported vulnerabilities, and the "detect" recommendation from NIST (2018), which sets up clear requirements for submission of identified vulnerabilities. The submission process should be encrypted in both directions, in order to protect the data transmitted between sender and receiver (HackerOne, 2017). While Laska et al. (2018) established submission guidelines, they were quite specific and not easily transferrable to diverse situations. How the organization with the vulnerable system reacts to, and responds to submission of the vulnerability disclosure is an essential component of the process (Takanen, Vuorijärvi, Laakso, & Röning, 2004). HackerOne (2017) concurs and notes the importance of clearly stating a commitment to resolving the vulnerability once it is verified as significant. Delayed responses, or lack of responses, may lead the discloser to publish immediately or to never report again.

All submissions are not equal in terms of criticality. Some submissions will be more or less critical than others. Thus, after submission, organizations need to consider how they will verify the vulnerability and assess its criticality. Along with setting guidelines for submissions, the verification comprises a portion of the "detect" component of NIST (2018). Verifying that the vulnerability exists and responding to the sender also matches ISO 29147 (2014) recommendations.

2.5.3 Restrictions

Laszka et al. (2018) recommended the inclusion of disclosure restrictions, legal clauses, and other prohibited, restricted, and unwanted activities; ISO/IEC 29147 (2014) agrees, recommending that organizations set restrictions on how and in what manner vulnerabilities will be disclosed, by both the organization and the reporter. Setting restrictions on external disclosure protects the organization until a resolution is found, corresponding to NIST (2018) recommendations. Further, we suggest that the "protect" component of NIST should offer limited liability to the researcher who in good faith, discovers and reports the vulnerability; this

corresponds to the "safe harbor" recommended by HackerOne (2017) and others, absolving cybersecurity professionals of criminal and civil liability for making the report, as long as both parties to the agreement follow the contract stipulations.

2.5.4 Credit

We added a category that specifically identifies the credit or recognition that the discloser will receive, following Laska et al.'s (2018) recommendations. Cybersecurity researchers may be more familiar with mechanisms of disclosure defined as: "full vendor" or "immediate public" or "hybrid" (Cavusoglu, Cavusoglu, & Raghunathan, 2007; HackerOne, 2017), and the CVD policy should specifically outline how the organization will give public credit to the cybersecurity researcher. ISO 29147 (2014) includes a debriefing session after the organization remediates the vulnerability, which may be included in the credit category. Awarding credit often comes at the end of the cycle, after the organization has gone through NIST's (2014) "respond" recommendation.

Preferences are another essential component of CVD policies (HackerOne, 2017), and we merged those components into the credit section; these requirements are also part of the "protect" and "respond" NIST (2018) sections, in that the organization protects its interests until a resolution is found, and then reports the resolution to the appropriate group(s). It may not be necessary to report to the public at large, but every effort should be made to make reports public to strengthen the nation's overall critical infrastructures. Credit should be given in a reasonable amount of time, as determined by the organization and the cybersecurity researcher.

2.5.5 Bounty

The fifth category for CVD is the expected benefit to the person who reports the vulnerability. We described the reward offered to those who disclose (if any) in the bounty category. In the past, cybersecurity researchers did not always expect bounties; however, that trend is changing

(Householder, Wassermann, Manion, & King, 2017). At the debriefing session, a bounty may or may not be awarded, and the bounty may be public or undisclosed, as part of the ISO 29147 (2014) recommendations. The bounty category corresponds to the fifth and final "recover" recommendation of NIST (2018). Bounties do not need to be financial; sometimes, public recognition is valuable enough to provide an incentive to cybersecurity researchers.

3. Method

3.1 Coordinated vulnerability disclosure policies of U.S. southeastern municipalities

We planned to analyze CVD policies from a representative sample of seven southeastern states in the United States: Alabama, Georgia, Mississippi, North Carolina, South Carolina, Tennessee, and Virginia, the same seven states whose laws on cybersecurity we discussed earlier and summarized in Table 1. As we began our search, we kept running into the same problem; we could find no CVD policies for city, county or state municipalities. There were no email contacts, phone numbers or other ways of reporting technical or implementation vulnerabilities. A cursory search of other U.S. states found similar problems, although we did not complete an exhaustive search outside of the southeast. Then, with no CVD policies publicly available on the networks of EASs in the southeast, we turned to public organizations upon which to evaluate a framework for CVD. We chose businesses we identified as likely to have exemplary CVD policies, which could then be adapted for use by EAS authorities.

3.2 Vulnerability disclosure policies of U.S. top 10 technology firms

Since there were no public, easily accessible CVD policies, we sought inspiration from the industry side, looking at vulnerability disclosure policies of the top 10 most profitable technology firms, according to Fortune 500 (Griffith, 2015), as shown in Table 2. As leaders in the field, with an established base of customers, clear technical and technological knowledge, and likely to have experience with prior vulnerability reporting, we surmised that these policies

might provide opportunities for reuse as municipalities seek to take advantage of cybersecurity researchers' work in vulnerability research.

Table 2. Top 10 Technology Firms

Company	Rank
Apple	1
Amazon	2
Google	3
Microsoft	4
IBM	5
Dell	6
Intel	7
Hewlett Packard Enterprise	8
Cisco	9
AT&T	10

Note. Adapted from http://fortune.com/2015/06/13/fortune-500-tech/

4. Results – CVD Policies

4.1 CVD Policies of Southeastern U.S. municipalities

Our plan was to evaluate a sample of U.S. EAS CVDs, using the southeast as an initial study. However, to our knowledge, there are no publicly available CVD policies for the EASs in any of the southeastern U.S. states, cities, and municipalities that we chose to analyze. The lack of CVD policies is an issue that EAS authorities should address, and quickly. Without a sample of EAS CVDs, we decided to look at top-performing technology organizations, to provide a high-quality reference sample for the EASs in the area we studied.

4.2 CVD policies of top 10 technology firms

We analyzed the CVD policies of the top 10 technology organizations in the Fortune 500, as shown in Table 3. We selected these companies because of their technology and technical expertise and long-term success. As expected, unlike most organizations, and unlike the EASs in

the southeastern U.S., all 10 of the organizations have CVD policies in place. These policies were easy to find via the use of a popular search engine website. We divided the CVD policies into the proposed framework and evaluated each component, based on the information available on the organization's website. Links to each of the CVDs are included in Table 3. EASs may choose to use these examples and the framework provided to develop CVDs for use in their networks.

4.2.1 Eligibility

Eligibility describes who may be entitled to bug bounty awards and recognition for finding, reporting, and in some cases, assisting in vulnerability mitigation. Of the ten organizations we analyzed, almost all had generic eligibility requirements, defining as eligible to submit vulnerabilities: "researchers" (Apple), "security researchers" (Amazon, Microsoft, IBM, Apple), the "security research community" (Google), "developers" (AT&T), and "independent researchers" (IBM and Cisco). IBM and Cisco further defined the following as eligible: "industry groups, government organizations, and vendors" and "industry organizations, vendors, customer, and other sources concerned with product or network security," respectively. Google further stated that they would not accept 3rd party organizations as eligible for submissions. While Intel had the strictest eligibility requirements, requiring the researcher to meet age, country, and relationship requirements, Dell and Hewlett Packard Enterprises did not have any eligibility requirements listed. Even where not mentioned, organizations would likely follow the legal guidelines of the areas in which they operate, meaning, for instance, that disclosers to U.S. organizations are ineligible if they are from embargoed countries, such as North Korea and Iran. At no time did these companies mention the word "hack" or "hacker" when describing eligibility requirements. These companies are not paying for those who penetrate vulnerable systems without permission and with malicious intent; but instead, are seeking cybersecurity researchers

with legitimate interests in improving long-term organizational security, and with no malicious intent. Some organizations, such as AT&T, require the creation of an account before submitting a vulnerability report.

4.2.2 Submission and verification

Except for Cisco, who accepts submissions via phone (or secure email), and AT&T, who accepts submissions online or via email, all of the organizations stated that they would use a secure method of communication via email or a link, with some sort of encryption. Response times vary, however, with some organizations (Amazon, IBM, and Hewlett Packard Enterprises) not confirming if the organization will respond to the vulnerability report, although IBM does state that a response will be received if there they receive a qualifying vulnerability. Cisco notes they usually acknowledge vulnerability reports within 48 hours, with follow-up reports and communications as needed, while AT&T usually responds in one day. Dell promises a confirmation email within 48 hours, while Intel says that a member of their Product Support Team will contact to discuss the problem. Microsoft provides a response within 24 hours and may involve the researcher in efforts to overcome the vulnerability. Apple promises an automated response to acknowledge receipt of the vulnerability report, although they do not specify an initial response time frame. Amazon Web Services (AWS) and Google appear to place great value on vulnerability reports, with AWS promising a non-automated response within 24 hours, and Google promising that a security team will evaluate the report, going so far as to list the names of the team members. However, a deeper dive into the AWS policy states that a live person will only send a message to the researcher if they verify the vulnerability and they consider it important enough to warrant further discussion. However, AWS asks the researchers to contact them if they do not receive a response to the original submission within a day or two.

4.2.3 Restrictions

Many of the restrictions involve not making public any information regarding the vulnerability, until a resolution is found and implemented. AT&T has the longest and most detailed set of restrictions, with many exclusions and specific rules for public disclosure. Apple and IBM ask the researcher not to disclose publicly before allowing time to fix the vulnerability. Google asks the discloser not to disrupt other Google users and provides a detailed list of both qualifying and excluded vulnerabilities. Google also asks that the researcher not violate any other laws. AWS, Microsoft, IBM, Dell, and Intel discuss public disclosure and how and when the information will be released, often suggesting that the researcher and the organization work together. HP's restriction policy requires the researcher to report the vulnerability English, while Amazon Retail and Cisco are silent on specific language requirements.

4.2.4 Credit

Several organizations (Amazon Retail, IBM, HP, and Cisco) make no promises regarding potential credit for the vulnerabilities disclosed. Apple, AWS, and Google describe coordinated plans for public disclosure and credit, after a patch is developed. Microsoft says that credit to the researcher is possible, using CVD policies, with the researcher following "environmentally safe" methods of releasing information about a vulnerability. Dell, Intel, and AT&T provide some sort of credit to the researcher, such as a link that credits all researchers who have found previous vulnerabilities, other online recognition, or other appropriate recognition at the organization's discretion.

In general, organizations prefer that cybersecurity researchers coordinate the vulnerability disclosure with them.

4.2.5 Bounty

If cybersecurity researchers discover a bug that has a large impact on organizations, they may receive a bounty for reporting the vulnerability. While some cybersecurity researchers may

envision a large financial reward for discovering and reporting a vulnerability, most vulnerabilities found are small in scope, with limited rewards. In fact, Apple, Amazon Retail, IBM, Dell, HP, and Cisco do not report information on potential bug bounties. Microsoft does not publish a specific bounty but only mentions that rewards are possible. AT&T reports that bounties are only applicable to public-facing environments, including websites, API, applications, and devices. AWS encourages researchers to use the Common Vulnerability Scoring System to evaluate possible bounties, while Google uses the Vulnerability Reward Program, with bounties from $100 to over $30,000, and Intel reports potential bounties of $500-$250,000.

The top 10 technology companies do an excellent job of explaining how to report vulnerabilities, with encrypted options to protect any messages that cybersecurity researchers send. Most organizations prefer a coordinated disclosure policy, where both the researcher and the impacted company release the vulnerability and the patch at the same time. This coordinated disclosure policy lessens the possibility of malicious actors profiting from the vulnerability before mitigation and resolution. By using the features of the top technology firms and the components identified, we propose a CVD process that EAS authorities may implement, to provide a more secure, stable, and reliable method of securing EASs and informing relevant constituents of emergencies.

5. Implications and Discussion

EASs, which offer significant opportunities for helping and informing people during an emergency, have an obvious need to ensure that the information that they share with the public is reliable, accurate, valid, and complete. As EAS authorities face the challenges associated with a fragmented, inconsistent, and scattered public-private-government supply chain, vulnerabilities are inevitable. While CVD policies may help to identify vulnerabilities in EASs, we could not

find any such policies for the U.S. southeastern states that we reviewed, using typical search engine tools. If EASs do not offer a method of reporting identified vulnerabilities, the cybersecurity researcher, who enjoys the non-routinized work of solving a problem, may give up, not report the vulnerability, and move to the next problem. Even worse, the cybersecurity researcher might choose to exploit the vulnerability, behaving in unethical and illegal ways. Alternatively, the cybersecurity researcher may attempt to report the vulnerability responsibly. However, without CVD policies, the researcher is fumbling in the dark, trying to guess how to report while maintaining ethical standards and not violating existing local, state, or federal laws. Meanwhile, the public served by the EAS may lose confidence after reports of the zombie apocalypse or emergency sirens blaring in the middle of the night without reason.

Since we could not review any CVDs for EASs, we developed a framework based on ISO and NIST standards, and previous research. We then used this framework to evaluate the top ten technology organizations based on five components: eligibility; submission and verification; restrictions; credit; and bounty. From this framework, we recommend a mutually beneficial method of linking EAS authorities with cybersecurity researchers. While we cannot prove that a CVD policy will identify every system vulnerability, prior research has shown that organizations without a CVD policy are at increased risk if a researcher finds a vulnerability (Reynolds, 2018). Moreover, numerous public successes have been reported with CVD policies, including bug bounty programs through the U.S. Armed Services and with organizations using Luta Security, HackerOne or other third-party vendors to manage their vulnerability disclosure programs. Some high-performing technology organizations, such as Google, seek strong and positive partnerships with the cybersecurity researcher community. Google notes they have: "…long enjoyed a close relationship with the security research community. To honor all the cutting-edge external

contributions that help us keep our users safe, we maintain a Vulnerability Reward Program for Google-owned web properties, running continuously since November 2010" (Google Vulnerability Reward Program (VRP) Rules, n.d.). EAS authorities should strive for the tight-knit community of cybersecurity research partners that Google and other top-performing technology companies have cultivated.

Easy to find CVD policies, that describe how to apply, who is eligible, the restrictions on submissions, and how credit and recognition will be handled, as proposed in the framework we presented, may resolve a vulnerability before systems are compromised, and in the case of EASs, before people are harmed. When designing CVD policies, we encourage EASs to keep the eligibility requirements as open as possible to gain benefit from the large pool of cybersecurity researchers, who may call themselves by many different occupational titles. At the same time, the organization does not want to promise too much and then spend substantial time on trivial vulnerabilities or invalid reports of vulnerabilities. We also recommend setting eligibility standards that keep the field open while aligning with any relevant laws, rules, and regulations. We found that organizations generally prefer cybersecurity researchers to submit vulnerability reports using encrypted methods of communication. We also found that some, but not all, organizations promise a response to the researcher. We encourage EAS authorities to require the use of encryption in all vulnerability report-related communications and to always respond to those who report a vulnerability, even if the response they automate the response. After receiving a vulnerability report, top organizations often set restrictions on the researchers, to allow time to verify the vulnerability and release a patch before informing the public. If the researcher agrees to a coordinated vulnerability process, they are more likely to receive credit and a potential bounty for the vulnerability reported; EAS authorities could implement a similar method of

awarding credit to those who make reports, and who agree to coordinated disclosure of the vulnerability, but only after they release a patch.

EAS authorities should review past responses to vulnerabilities disclosed, learn from them, and develop CVD policies to lessen the chance of similar occurrences in the future. EAS authorities should welcome cybersecurity researchers and allow them to scan for vulnerabilities and disclose privately, to the organization, without fear of reprisal. In this way, EAS authorities set the rules, and cybersecurity researchers have explicit bounds on their testing, all working together to protect the public from known system vulnerabilities.

6. Limitations and Future Research

Our study is not without limitations. More generation and testing of theoretical foundations of CVD policies is an important avenue of future research. Our study adds to the body of knowledge to increase the maturity of CVD policies for EASs, but we did not test an implementation of the recommendations. We described methods to improve resilience, strengthen public-private-government partnerships, adopt appropriate CVD policies, and increase the security of only one particular critical infrastructure system – the EAS, providing a specific context. We developed a framework based on ISO and NIST standards, which EAS authorities could use as a starting point for development of publicly available, easily found CVD policies, encouraging more collaborative efforts between information security researchers and organizations that are part of the EAS network. Future researchers will no doubt find it difficult to test the effectiveness of CVD policies because of the secrecy shrouding national critical infrastructure, including the EAS.

While Laszka et al. (2018) considered one specific bug bounty program, we developed a more generalized framework for CVD policies for EASs. Further refinement of the criteria for developing CVD policies could include the addition of bug bounty platforms, along with the

inclusion of CVD policies from additional organizations. Since we used Fortune 500 companies to assess the proposed framework, we did not include private companies in our discussion. Further, since we selected the top ten most successful technology organizations, what might the bottom ten show? Or the middle tier? Future research could also analyze all organizations and not focus on technology companies and could compare those organizations with CVD policies to those which do not have a CVD policy. Which of those organizations receives more tips on vulnerabilities? How does having a CVD policy affect organizational performance? Understanding how different CVD policies affect the relationship between organizations and cybersecurity researchers could help to test further the framework we proposed. All of this future work could help to build upon the burgeoning field of vulnerability disclosure and how organizations respond to them.

Moreover, while we focused on organizational-level implications for the development of CVD policies, we did not survey end users, as recommended by Karlsson et al. (2016). Since they are the ones who ultimately make the system work, assessing their attitudes and perceptions of system vulnerabilities, and gathering their input into possible remedies, would be informing. While previous researchers have noted the importance of adequately training employees in security techniques, we did not investigate the impact of training on the development, implementation, and enforcement of CVD policies.

We analyzed the vulnerability disclosure policies for EASs in one particular location: the southeast U.S. Examination of different portions of the U.S. may lead to different interpretations regarding the maturity of vulnerability disclosure policies. Perhaps, for instance, the west, northeast or midwest areas of the U.S. differ regarding publishing vulnerability disclosure

policies. Outside the U.S., other countries may have very different methods of alerting the population, with different priorities.

Our focus on one particular instance of critical infrastructure – the EAS – may limit the external generalizability of our recommendations to other portions of the national critical infrastructure. An analysis of CVD policies in other governmental organizations, such as the armed services, might lend further insight on how to use management policies to improve the resilience of the interconnected network of technological systems such as water, power, and gas for example. Expansion to public and private non-governmental agencies might also present compelling information. Since most portions of critical infrastructure are privately owned, understanding how small – but crucial – portions of critical infrastructure interact with each other, provides opportunities to improve the security of EASs.

7. Conclusion

It would be a shame if the zombie apocalypse was about to happen, and because of a system vulnerability, EASs did not alert us. In that hypothetical situation, perhaps a cybersecurity researcher identified a vulnerability weeks, days, or hours before. Further, that researcher operates in the U.S., where scanning of another's system without permission may be punishable by criminal penalties, regardless of intent. Thus, the fear of legal reprisals, along with a lack of a CVD policy, may lead to non-disclosure of the vulnerability. Even more troubling, perhaps a researcher reports the vulnerability, but the organization does not remediate it, putting the groups served at risk. We suggest instead that the cybersecurity researcher read all CVD policies before investigating vulnerable systems and ensure compliance with the policies.

Further, we recommend that government authorities at all levels work to oppose laws that restrict public-private-government partnerships by criminalizing cybersecurity research with no harmful

intent. EASs as a whole must be resilient. EAS authorities need to recognize that vulnerabilities will occur, but that they can mitigate exposure by using the expertise of cybersecurity researchers. As discussed, the system is only as strong as the weakest link. To reduce vulnerabilities, EAS authorities need to develop CVD policies. A bottom-up approach, starting at the local level and moving to the state, for instance, is one option. A top-down approach, letting the states take the lead and moving down to local, city, and county municipalities, is also an acceptable approach. We suggested a taxonomy of items to consider as organizations develop a CVD policy, including who is eligible, how to submit, restrictions, giving credit to the researcher, and a bounty, if applicable. Our aging, vulnerable EAS is vulnerable to potential threats, and EAS authorities lack the proper budget to find all the vulnerabilities. Using the army of cybersecurity researchers and writing a good CVD policy will strengthen the U.S. emergency alert systems, which benefits society.

8. References

6 U.S. Code § 321o. (2016). Integrated public alert and warning system modernization *Legal Information Institute*, U.S. Code Title 6. Domestic Security, Chapter 1, Homeland Security Organization, Subchapter V, National Emergency Management, Section 321o. Integrated public alert and warning system modernization. https://www.law.cornell.edu/uscode/text/6/321o

47 U.S. Code § 606 - War Powers of President. (n.d.). U.S. Code › Title 47 › Chapter 5 › Subchapter VI › § 606. Retrieved from https://www.law.cornell.edu/uscode/text/47/606 Accessed 24 January 2019.

AL Code § 13A-8-13. (n.d.). Alabama Computer Crime Act. *Internet Library of Law and Court Decisions*. http://www.internetlibrary.com/statuteitem.cfm?Num=10#103

Attrition. (2016). *Legal threats against security researchers: How vendors try to save face by stifling legitimate research.* Retrieved from http://attrition.org/errata/legal_threats/ Accessed 24 January 2019.

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy & Security, 8*(2), 33-56.

Baudoin, M. A., Henly-Shepard, S., Fernando, N., Sitati, A., & Zommers, Z. (2016). From top-down to "community-centric" approaches to early warning systems: Exploring pathways to improve disaster risk reduction through community participation. *International Journal of Disaster Risk Management, 7*(2), 163-174. doi:https://doi.org/10.1007/s13753-016-0085-6.

Bonderud, D. (2014). The responsible disclosure policy: Safeguard or cybercriminal siren song? *SecurityIntelligence (Brought to you by IBM).* Retrieved from https://securityintelligence.com/the-responsible-disclosure-policy-safeguard-or-cybercriminal-siren-song/ Accessed 24 January 2019.

Borchert, H. (2015). It takes two to tango: Public-private information management to advance critical infrastructure protection. *European Journal of Risk Regulation: EJRR, 6*(2), 208-218.

Branscombe, M. (2017). How to handle security vulnerability reports. *Cio.com*. Retrieved from https://www.cio.com/article/3157698/security/how-to-handle-security-vulnerability-reports.htmlf Accessed 24 January 2019.

Brem, S. (2015). Critical infrastructure protection from a national perspective. *European Journal of Risk Regulation (EJRR), 6*(2), 191-199.

Brinson, S. L. (2009). CONELRAD on the front line of Cold War defense. *Media, War & Conflict, 2*(3), 339-357.

Calabrese, C. (2017). “The cyber” part II: Cybersecurity research and the role of the enforcer. *Center for Democracy and Technology (CDT) (online)*. Retrieved from https://cdt.org/blog/the-cyber-part-ii-cybersecurity-research-and-the-role-of-the-enforcer/ Accessed 24 January 2019.

Carter, J. G., Carter, D. L., Chermak, S., & McGarrell, E. (2017). Law enforcement fusion centers: Cultivating an information sharing environment while safeguarding privacy. *Journal of Police and Criminal Psychology, 32*(1), 11-27. doi: 10.1007/s11896-016-9199-4

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2007). Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge. *IEEE Transactions on Software Engineering, 33*(3), 171-185. doi: https://ieeexplore.ieee.org/document/4084135

Claus, B., Gandhi, R. A., Rawnsley, J., & Crowe, J. (2015). Using the oldest military force for the newest national defense. *Journal of Strategic Security, 8*(4), 1-22. doi:10.5038/1944-0472.8.4.1441

Clayton, M. (2011). Did national emergency alert system play Lady Gaga? *Christian Science Monitor*. Retrieved from http://www.nbcnews.com/id/45225452/ns/us_news-security/t/did-national-emergency-alert-system-play-lady-gaga/#.W-40MZNKg5M Accessed 24 January 2019.

Coalition. (2016). Coalition Launches Surveys to Investigate Perspectives on Vulnerability Disclosure and Handling: Calls for Public Participation from Technology Providers, Operators, and Security Researchers. *NASDAQ OMX's News Release Distribution Channel*.

Cohen, W. J., & Boyer, E. F. (1951). Federal Civil Defense Act of 1950: Summary and legislative history. *Social Security Bulletin, 14*, 11.

Condit, J. (2018). Arkansas National Guard Conducts Cyber Training Exercise. *U.S. Department of Defense*. Retrieved from https://www.defense.gov/News/Article/Article/1408321/ Accessed 24 January 2019.

Constantin, L. (2013). Emergency alert system devices vulnerable to hacker attacks, researchers say. *ComputerWorld (online)*. Retrieved from https://www.computerworld.com/article/2494934/malware-vulnerabilities/emergency-alert-system-devices-vulnerable-to-hacker-attacks--researchers-say.html Accessed 24 January 2019.

Conway, M. (2006). The birth of CBS-TV News: An ambitious experiment at the advent of U.S. commercial television. *Journalism History, 32*(3), 128-137.

Crown, E. (2017). 'Hacking for Defense' students team with Army to improve casualty care triage. *U.S. Army, Medical Materiel Agency*. Retrieved from https://www.army.mil/article/193463/hacking_for_defense_students_team_with_army_to_improve_casualty_care_triage Accessed 24 January 2019.

Davis, M. (2015). Developers: How do you respond to security researcher's vulnerability reports? *Future Hosting (futurehosting.com)*. Retrieved from https://www.futurehosting.com/blog/developers-how-do-you-respond-to-security-researchers-vulnerability-reports/ Accessed 24 January 2019.

Diaz, J. (2012). This message from NORAD announced global nuclear war—In 1971. *Gizmodo.com*. Retrieved from https://gizmodo.com/5923528/this-message-from-norad-announced-world-nuclear-war-in-1971 Accessed 24 January 2019.

Dittmer, J., & Wright, B. (n.d.). Minimizing legal risk when using cybersecurity scanning tools. *SANS Institute InfoSec*. Retrieved from https://www.sans.org/reading-room/whitepapers/legal/paper/37522 Accessed 24 January 2019.

Dixon, H. B., Jr. (2018). Cyberattacks on courts and other government institutions. *The Judges' Journal, 57*(3), 37-39

DoD News. (2016). 'Hack the Pentagon' pilot program opens for registration. *U.S. Department of Defense*. Retrieved from https://www.defense.gov/News/Article/Article/710033/hack-the-pentagon-pilot-program-opens-for-registration/ Accessed 24 January 2019.

DoD Vulnerability Disclosure Policy. (2016). HackerOne. Retrieved from https://hackerone.com/deptofdefense Accessed 24 January 2019.

Dodril, T. (2016). Emergency alert system vulnerabilities could allow terrorists to manipulate a disaster. *SurvivalBased.com*. Retrieved from http://www.survivalbased.com/survival-blog/7229/emergency-alert-system-vulnerabilities-could-allow-terrorists-to-manipulate-a-disaster/ Accessed 24 January 2019.

Domdouzis, K., Akhgar, B., Andrews, S., Gibson, H., & Hirsch, L. (2016). A social media and crowdsourcing data mining system for crime prevention during and post-crisis situations. *Journal of Systems and Information Technology, 18*(4), 364-382. doi:https://doi.org/10.1108/JSIT-06-2016-0039

Egli, D. S. (2013). Beyond the storms: Strengthening preparedness, response, & resilience in the 21st century. *Journal of Strategic Security, 6*(2), 32-45. doi:10.5038/1944-0472.6.2.3

Eichensehr, K. E. (2017). Public-private cybersecurity. *Texas Law Review, 95*(3), 467-538.

Emergency notification system definitive guide. (n.d.). Keep your people safe, informed, and connected. *Alert Media*. Retrieved from https://www.alertmedia.com/emergency-notification-system Accessed 24 January 2019.

Fakhoury, H. (2014). Appeals Court overturns Andrew "weev" Auernheimer conviction – important decision impacts constitutional rights in the Internet Age. Retrieved from https://www.eff.org/press/releases/appeals-court-overturns-andrew-weev-auernheimer-conviction Accessed 24 January 2019.

Federal Communications Commission (FCC). (2018). Emergency Alert System (EAS). Retrieved from https://www.fcc.gov/consumers/guides/emergency-alert-system-eas Accessed 24 January 2019.

FEMA Fact Sheet. (2007). Emergency Alert System and Notification (archive). Retrieved from https://web.archive.org/web/20070717212239/http://www.fema.gov/media/fact_sheets/eas.shtm Accessed 24 January 2019.

Finifter, M., Akhawe, D., & Wagner, D. (2013). An empirical study of vulnerability rewards programs. *Proceedings of the 22nd USENIX Security Symposium*.

FL Code § 815.06 (2019). Title XLVI, Crimes. Chapter 15, Computer-related crimes. 815.06 Offenses against users of computers, computer systems, computer networks, and electronic devices. *2019 Florida Statutes*. http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0800-0899/0815/0815.html

Ga. Code § 16-9-90 to 16-9-157. Title 16, Crimes and Offense, Chapter 9, Forgery and Fraudulent Practices, Article 6, Computer Systems Protection, Part 1, Computer Crimes. *Georgia General Assembly, Official Code of Georgia Annotated*.

Gallagher, S. (2018). Georgia governor vetoes cyber bill that would criminalize "unauthorized access". *Ars Technica*. Retrieved from https://arstechnica.com/tech-policy/2018/05/georgia-governor-vetoes-cyber-bill-that-would-criminalize-unauthorized-access/ Accessed 24 January 2019.

Goff, J. (2017). Prospective vigilance: Assessing complex coordinated attack preparedness programs. *Homeland Security Affairs*. Naval Postgraduate School, Monterey, CA. https://www.hsaj.org/resources/uploads/2014/12/pdf.png

Google Vulnerability Reward Program (VRP) Rules, (n.d.). *Google.* Retrieved from https://www.google.com/about/appsecurity/reward-program/ Accessed 24 January 2019.

Green, A. (2018). Google and Microsoft ask Governor Deal to veto SB 315. Retrieved from https://blog.andy-green.org/2018/04/25/tech-giants-google-and-microsoft-ask-gov-deal-to-veto-sb-315/

Griffith, E. (2015). *The top technology companies of the Fortune 500*. Retrieved from Fortune: http://fortune.com/2015/06/13/fortune-500-tech/ Accessed 24 January 2019.

Hack the Pentagon. (n.d.). Hackerone. Retrieved from https://www.hackerone.com/resources/hack-the-pentagon Accessed 24 January 2019.

HackerOne. (2017). Vulnerability disclosure policy basics: 5 critical components. *h:blog (online)*.

Hausken, K. (2017). Security investment, hacking, and information sharing between firms and between hackers. *Games, 8*(2), 23. doi:10.3390/g802002

Hemme, K. (2015). Critical infrastructure protection: Maintenance is national security. *Journal of Strategic Security, 8*(5), 25-39. doi:10.5038/1944-0472.8.3S.1471

Householder, A. D., Wassermann, G., Manion, A., & King, C. (2017). *The CERT® guide to coordinated vulnerability disclosure.* CERT Division, Special Report: CMU/SEI-2017-SR-022. Software Engineering Institute, Carnegie Mellon University.

Hub. (2017). Hackers put the entire city of Dallas on alert. *Hub (online)*. Retrieved from https://www.hubinternational.com/blog/2017/04/hackers-put-the-entire-city-of-dallas-on-alert/ Accessed 24 January 2019.

ISO/IEC 29147. (2014). Information technology — Security techniques — Vulnerability disclosure. International Standard. Retrieved from http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip Accessed 24 January 2019.

ISO/IEC 30111. (2013). Information technology — Security techniques — Vulnerability handling processes International Standard. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:30111:ed-1:v1:en Accessed 24 January 2019.

Jump, M. (2019). Fighting cyberthreats with technology solutions. *Biomedical Instrumentation & Technology, 53*(1), 38-43.

Kang, C. (2018). False missile warning in Hawaii adds to scrutiny of emergency alert system. *The New York Times*. Retrieved from https://www.nytimes.com/2018/01/13/business/hawaii-missile-emergency-alert.html Accessed 24 January 2019.

Karlsson, F., Kolkowska, E., & Prenkert, F. (2016). Inter-organisational information security: A systematic literature review. *Information and Computer Security, 24*(5), 418-451.

Kosseff, J. (2018). Defining cybersecurity law. *Iowa Law Review, 103*(3), 985-1031.

Kranenbarg, M. W., Holt, T. J., & van der Ham. J. (2018). Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure. *Crime Science, 7*(1), 1-9.

Krebs, B. (2014). Target hackers broke in via HVAC company. *KrebsOnSecurity*. Retrieved from https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ Accessed 24 January 2019.

Kubitschko, S. (2015). The role of hackers in countering surveillance and promoting democracy. *Media and Communication, 3*(2). doi:http://dx.doi.org/10.17645/mac.v3i2.281

Laszka, A., Zhao, M., Malbari, A., & Grossklags, J. (2018). The rules of engagement for bug bounty programs. *Financial Cryptography and Data Security*.

Lechner, N. H. (2017). An overview of cybersecurity regulations and standards for medical device software. *Proceedings of the Central European Conference on Information and Intelligent System*, 237-249.

Li, D. C. (2015). Online security performances and information security disclosures. *The Journal of Computer Information Systems, 55*(2), 20-28.

Lynch, S. (2016). Full disclosure: Infosec industry still fighting over vulnerability reporting. *Cisco Umbrella*. Retrieved from https://umbrella.cisco.com/blog/2015/10/16/full-disclosure-infosec-industry-still-fighting/ Accessed 24 January 2019.

Manley, M. (2015). Cyberspace's dynamic duo: Forging a cybersecurity public-private partnership. *Journal of Strategic Security, 8*(5). doi:10.5038/1944-0472.8.3S.1478

Marett, K. (2015). Checking the manipulation checks in information security research. *Information and Computer Security, 23*(1), 20-30.

Mason, J. (2018). Cyber security statistics. *The Best VPN (online)*. Retrieved from https://thebestvpn.com/cyber-security-statistics-2018/ Accessed 24 January 2019.

Matwyshyn, A. M. (2013). Hacking speech: Informational speech and the First Amendment. *Northwestern University Law Review, 107*(2), 795-845.

Matwyshyn, A. M. (2017). CYBER! *Brigham Young University Law Review, 2017*(5), 1109-1195.

McFarlane, R. (2017). Hacking emergency services: How safe is the 911 system? . *GCN.com*. Retrieved from https://gcn.com/articles/2017/07/18/hacking-emergency-services.aspx

McGuire, M. (2018). Beyond flatland: When smart cities make stupid citizens. *City, Territory and Architecture, 5*(1), 1-11. doi:10.1186/s40410-018-0098-0

Meshkati, N., & Tabibzadeh, M. (2016). An integrated system-oriented model for the interoperability of multiple emergency response agencies in large-scale disasters: Implications for the Persian Gulf. *International Journal of Disaster Risk Science, 7*, 227-244. doi:10.1007/s13753-016-0099-0

Metivier, B. (2017). Fundamental objectives of information security: The CIA triad. *Sage Data Security*. Retrieved from https://www.sagedatasecurity.com/blog/fundamental-objectives-of-information-security-the-cia-triad Accessed 24 January 2019.

Michigan. (2018). Michigan Cyber Defense Corps. Retrieved from https://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---,00.html Accessed 24 January 2019.

Miron, W., & Muita, K. (2014). Cybersecurity capability maturity models for providers of critical infrastructure. *Technology Innovation Management Review, 4*(10), 33-39.

Morgan, S. (2015). The business of cybersecurity: 2015 market size, cyber crime, employment, and Industry statistics. *Forbes.com (online)*. Retrieved from https://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/#3557a6fe5d0d Accessed 24 January 2019.

Morrison, M. I. (2013). The acquisition supply chain and the security of governmental information technology purchases. *Public Contract Law Journal, 42*(4), 749-792.

Nakashima, E., & Soltani, A. (2014). The ethics of hacking 101 (posted 2014-10-08 03:20:38). *The Washington Post (online)*.

Nasu, H. (2015). State secrets law and national security. *The International and Comparative Law Quarterly, 64*(2), 365-404. doi:10.1017/S0020589315000056

N.C. Gen. Stat. § 14-453 to 14-458. Chapter 14, Article 60, Computer-Related Crime. (n.d.). *North Carolina Legislature, Enacted Legislation*. https://www.ncleg.net/EnactedLegislation/Statutes/HTML/ByArticle/Chapter_14/Article_60.html

NIST (2018). National Institute of Standards and Technology, Version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Network Installation v. VC3. (2000). Scott Alan Moulton and Network Installation Computer Services, Inc., Plaintiffs, v. VC3, Defendant. Northern District of Georgia. Retrieved from http://www.internetlibrary.com/pdf/Moulton-VC3.pdf Accessed 24 January 2019.

Nixon, R. (2016). Homeland Security Dept. struggles to hire staff to combat cyberattacks. *The New York Times*. Retrieved from https://www.nytimes.com/2016/04/07/us/politics/homeland-security-dept-struggles-to-hire-staff-to-combat-cyberattacks.html Accessed 24 January 2019.

Norris, D., Joshi, A., & Finin, T. (2015). Cybersecurity challenges to American state and local governments. *European Conference on e-Government: Academic Conferences International*, Kidmore End, 196-202.

Occupational Employment Statistics (2017). 15-1122 Information Security Analysts. May 2017 National Occupational Employment and Wage Estimates. *U.S. Department of Labor, Bureau of Labor Statistics*. https://www.bls.gov/oes/2017/may/oes_nat.htm

Ollmann, G. (2013). Hacking the emergency alerting system. *Information Week - DARKReading (online)*. Retrieved from https://www.darkreading.com/attacks-breaches/hacking-the-emergency-alerting-system/d/d-id/1140113 Accessed 24 January 2019.

Osborne, C. (2016). Security researcher arrested for disclosing US election website vulnerabilities. Zero Day. *Zdnet.com*. Retrieved from http://www.zdnet.com/article/security-researcher-arrested-for-reporting-us-election-website-vulnerabilities/ Accessed 24 January 2019.

Peeters, G. (2017). Strengthening the Achilles heel of the European Union: Make use of ethical hackers to find vulnerabilities in information systems? *Leiden University Repository, Masters Thesis*. Retrieved from https://openaccess.leidenuniv.nl/bitstream/handle/1887/55426/Masterthesis%20Gijs%20Peeters%20S1584103%20%5bJuly%202017%20final%5d.pdf?sequence=1 Accessed 24 January 2019.

Peterson, A. (2015). This ’80s-era criminal hacking law scares cybersecurity researchers. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2015/08/05/this-80s-era-criminal-hacking-law-scares-cybersecurity-researchers/?utm_term=.ec5f5a2f0fae Accessed 24 January 2019.

Raab, C. D., Jones, R., & Székely, I. (2015). Surveillance and resilience in theory and practice. *Media and Communication, 3*(2). doi:10.17645/mac.v3i2.220

Reuters. (2013). Zombie hack blamed on easy passwords. *Chicago Tribune (online)*. Retrieved from http://articles.chicagotribune.com/2013-02-14/business/chi-zombie-hack-blamed-on-easy-passwords-20130214_1_karole-white-ioactive-labs-passwords Accessed 24 January 2019.

Reynolds, C. (2018). *Vulnerability Disclosure Not a Priority for 93% of Forbes Global 2000.* Retrieved from https://www.cbronline.com/news/vulnerability-disclosure-policies Accessed 24 January 2019.

Roberts, Paul. (2013). Emergency alert system: Vulnerable systems double, despite zombie hoax. *The Security Ledger*. Retrieved from https://securityledger.com/2013/07/emergency-alert-system-vulnerable-systems-double-despite-zombie-hoax/ Accessed 24 January 2019.

Rodin, D. N. (2015). The cybersecurity partnership: A proposal for cyberthreat information sharing between contractors and the federal government. *Public Contract Law Journal, 44*(3), 505-528.

Sales, N. A. (2013). Regulating cyber-security. *Northwestern University Law Review, 107*(4), 1503-1568.

Sangster, J. L. (2008). Are southern states better positioned for technology projects? *Area Development (online)*. Retrieved from http://www.areadevelopment.com/specialPub/southernTech08/southern-states-technology-projects.shtml Accessed 24 January 2019.

S.C. Code § 16-16-10 to 16-16-40. Title 16 – Crimes and Offenses, Chapter 16 – Computer Crime Act. *South Carolina Code of Laws Unannotated*. https://www.scstatehouse.gov/code/t16c016.php

Seals, T. (2017). Hack the Air Force 2.0 bug bounty kicks off with $10K payout. *Infosecurity*. Retrieved from https://www.infosecurity-magazine.com/news/hack-the-air-force-20-bug-bounty/ Accessed 24 January 2019.

Signal. (n.d.). Defense Department launches 'Hack the Army' bug bounty program. Retrieved from https://www.afcea.org/content/Blog-defense-department-launches-hack-army-bug-bounty-program Accessed 24 January 2019.

Storm, D. (2013). Hackers can hijack unpatched emergency alert system devices, broadcast bogus warnings. *ComputerWorld (online)*. Retrieved from https://www.computerworld.com/article/2473992/malware-vulnerabilities/hackers-can-hijack-unpatched-emergency-alert-system-devices--broadcast-bogus.html Accessed 24 January 2019.

Suárez, R. A., & Scott, D. (2017). Doing what is right with coordinated vulnerability disclosure. *Biomedical Instrumentation & Technology*, 42-45.

Takanen, A., Vuorijärvi, P., Laakso, M., & Röning, J. (2004). Agents of responsibility in software vulnerability processes. *Ethics and Information Technology, 6*(2), 93-110.

Tenn. Code Ann. § 39-14-602 (2018). Title 39 - Criminal Offenses, Chapter 14 - Offenses Against Property, Part 6 - Tennessee Personal and Commercial Computer Act of 2003, § 39-14-

602. Violations – Penalties. *Justia US Law*. https://law.justia.com/codes/tennessee/2018/title-39/chapter-14/part-6/section-39-14-602/

USAJobs. (2018). Information technology program manager (Policy and planning/information security). *Department of the Army*. Retrieved from https://www.usajobs.gov/GetJob/ViewDetails/495022600 Accessed 24 January 2019.

Va. Code § 18.2-152.1 to 152.15. Virginia Computer Crimes Act. Title 18-2, Crimes and Offenses Generally, Chapter 5, Crimes against Property, Article 7.1, Computer Crimes. *Code of Virginia*. https://law.lis.virginia.gov/vacodefull/title18.2/chapter5/article7.1/.

Walker, J. J. (2012). Cyber Security Concerns. In B. Eksioglu (Ed.), *Emergency Management* (pp. 39-58). InTech. Retrieved from https://www.intechopen.com/books/emergency-management/cyber-security-concerns-for-emergency-management Accessed 24 January 2019.

What is Hacking for Defense, (n.d.). *H4Di.* Retrieved from https://www.h4di.org/about.html Accessed 24 January 2019.

Winkler, J. R. (2016). Blurred lines: National security and the civil-military struggle for control of telecommunications policy during World War II. *Information & Culture, 51*(4), 500-531. doi:10.7560/IC51403

Wirth, A. (2017). Cyberinsights: It's time for belts and suspenders. *Biomedical Instrumentation & Technology, 51*(4), 341-345.

Wolff, J., & Lehr, W. (2018). When cyber threats loom, what can state and local governments do? *Georgetown Journal of International Affairs*, 19, 67.

Wrona, K., Moye, T., Lagadec, P., Street, M., Lenk, P., & Jordan, F. (2018). Cybersecurity innovation in NATO: Lessons learned and recommendations. *Information & Security, 36*, 1-25. doi:10.11610/isij.3603

Yasin, R. (2016). So you want to be a security researcher?. *Information Week – DarkReading*. Retrieved from https://www.darkreading.com/careers-and-people/so-you-want-to-be-a-security-researcher/d/d-id/1324453 Accessed 24 January 2019.

Yerak, B. (2015). FBI seeking 'ethical' hackers. c. *Telegraph – Herald*, 89.

Zetter, K. (2016). Appeals Court overturns conviction of AT&T hacker 'Weev'. *Wired.com*. Retrieved from https://www.wired.com/2014/04/att-hacker-conviction-vacated Accessed 24 January 2019.

Table 3. Top 10 Tech Companies and Vulnerability Disclosure Policies

Company Rank & **URL of Disclosure Policy**	**Eligibility**	**Submission and verification**	**Restrictions**	**Credit**	**Bounty**
1 Apple https://support.apple.com/en-us/HT201220	Researchers	Dedicated encrypted email Will send automatic response via email; response time not indicated Will send additional emails if needed	Does not disclose, discuss, or confirm security issues until vulnerability is identified and resolved	Credit researchers after resolution	Not mentioned
2 Amazon **Amazon Retail** https://www.amazon.com/gp/help/customer/display.html?nodeId=201909140 **Amazon Web Services (AWS)** https://aws.amazon.com/security/vulnerability-reporting/	Security researchers Amazon retail and Amazon Web Services (AWS) handled separately	Amazon Retail Dedicated encrypted email Response time not indicated AWS Will send non-automated response within 24 hours, even if they determine there is not a vulnerability Progress updates promised at least every 5 working days	Amazon Retail None described Amazon Web Services Will send results and information about public disclosure	Amazon Retail Not described AWS Will coordinate public disclosure	Amazon Retail N/A Amazon Web Services Use version 2.0 of the Common Vulnerability Scoring System (CVSS) to evaluate potential vulnerabilities
3 Google	Security research community	Encrypted submission link	Do not disrupt other Google users	Coordinated public disclosure	Vulnerability Reward Program

Company Rank & URL of Disclosure Policy	Eligibility	Submission and verification	Restrictions	Credit	Bounty
https://www.google.com/about/appsecurity/reward-program/		Evaluated by Google Security Team	Only use your own Google accounts Detailed list of vulnerabilities that do/do not qualify Don't violate any other laws		Range from $100 to over $30k; Reward chart published List of vulnerabilities that do/do not qualify Does not reward disclosure through 3rd party firms No rewards to those in countries on sanctions list or who are themselves on sanctions lists
4 Microsoft https://technet.microsoft.com/en-us/security/dn467923.aspx	Security Researcher	Encrypted email Response within 24 hours Include as much information as possible about the vulnerability, including type of issue, impacts, products affected, etc.	Allow time to fix before disclosing publicly	Possibly Coordinated Vulnerability Disclosure	Unknown but reward is mentioned

Company Rank & URL of Disclosure Policy	Eligibility	Submission and verification	Restrictions	Credit	Bounty
		May interact with researcher as the problem is investigated and resolved			
5 IBM https://www.ibm.com/security/secure-engineering/report.html	Security researchers, industry groups, government organizations and vendors	Online or via secure email Response time not indicated Tech support will investigate and respond if there is a vulnerability	Inform if you want public recognition and your disclosure plans	Unknown	n/a
6 Dell http://www.dell.com/learn/us/en/04/campaigns/report-vulnerability	n/a	Secure email Will receive confirmation email within 48 hours	Would like to work together with the finder to disclose the vulnerability and mitigation	Will provide a link that credits all the researchers who have found previous vulnerabilities.	n/a
7 Intel https://security-center.intel.com/BugBountyProgram.aspx	Strict eligibility requirements – age, country, relative of Intel employee, etc.	Secure email Member of Product Support Team will contact to discuss the problem	Will disclose as agreed upon	Recognized online or as otherwise agreed upon	$500-$250k
8 Hewlett Packard Enterprise	None stated	Secure email or link	Only English language	n/a	n/a

Company Rank & URL of Disclosure Policy	Eligibility	Submission and verification	Restrictions	Credit	Bounty
https://www.hpe.com/us/en/services/security-vulnerability.html		Response time or process not indicated			
9 Cisco https://www.cisco.com/c/en/us/about/security-center/security-vulnerability-policy.html	Independent researchers, industry organizations, vendors, customers, and other sources concerned with product or network security	Secure email or by phone Usually acknowledged within 48 hours Ongoing status reports and communication as needed	n/a	n/a	n/a
10 AT&T https://bugbounty.att.com/	Developers and security researchers Only registered users	Online and/or via email Must sign-in to view Usually respond in 1 day	Described in detail Numerous exclusions and rules	Appropriate recognition at AT&T's discretion	Bug bounty program applies to public-facing environment including websites, API, applications, and devices.