THE CYBER DEFENSE REVIEW
A Joint Production of the Army Cyber Institute and Marine Corps Forces Cyber Command
http://www.cyberdefensereview.org

Army Vulnerability Response Program: A Critical Need in the Defense of our Nation

Categories : Articles

Date : October 23, 2015

Abstract: *Many major corporations have standing "bug bounty" programs that monetarily reward participants for identifying vulnerabilities in their products and responsibly disclosing the findings to the company. These programs help ensure vulnerabilities end up in the correct hands and lead to products that are more secure. In contrast, the Army does not have a central location for responsibly disclosing vulnerabilities found through daily use, much less a program that can permit active security assessments of networks or software solutions. Without a legal means to disclose vulnerabilities in Army software or networks, vulnerabilities are going unreported and unresolved. The critical necessity of an Army vulnerability response program will be highlighted throughout this paper as well as a proposed implementation to better defend our networks and sensitive information.*

Keywords: Bug bounty, responsible disclosure, network defense, information protection

Introduction:

On April 26, 2015, Secretary of Defense Ashton Carter met with experts from Silicon Valley in an attempt to build a partnership that could bolster the nascent cyber capabilities of the Department of Defense (DoD).[1] Secretary Carter recognized the Pentagon's use of legacy processes and lack of agility in adopting innovative ideas from start-ups and leaders within the technology industry. One such idea is the private sector's handling and remediation of responsibly disclosed vulnerabilities. Secretary Carter's historic visit occurred shortly after the public revelation of a high-profile case of Russian cyber espionage against the White House and Department of State which resulted in the exfiltration of unclassified Presidential emails.[2] The Russian hackers leveraged a publicly-known vulnerability in software running on the Pentagon network–a vulnerability for which a patch existed but administrators did not apply.[3] In the months that followed, the US government confirmed it had fallen victim to other nation-state exploits. Arguably the most significant publicly acknowledged compromise occurred when Chinese hackers gained access to computer systems within the Office of Personnel Management which hold sensitive records on current and previous federal employees. Once again, the adversary used a known, signatured, exploitation tool.[4] Had the U.S. Government implemented lessons learned and best practices from the private sector and utilized a functional "bug bounty" program, it is possible that many of these incidents could have been mitigated or even prevented. The U.S. Army urgently needs to stand up a vulnerability disclosure and response program that would permit its personnel to responsibly report findings to a centralized entity that would assist in tracking and resolving issues. The Army could construct such

an entity within existing frameworks and regulations with minimal overhead while drastically fortifying our digital defenses. A successful program within the Army would inevitably result in wide-scale adoption across the Department of Defense and U.S. Government.

Definitions:

To understand the problem at hand, it is critical to first review technology vulnerability terminology. A “bug” is a weakness within an application that causes the application to perform in an unexpected manner given certain conditions or inputs. Hackers can capitalize on this unexpected state using various exploitation techniques to gain unauthorized access to systems or information. Vulnerabilities within embedded systems and firmware are particularly dangerous because they are often utilized in critical infrastructure and key resources. Administrators often forego patching and updating these systems because they are non-redundant; the systems are a single point of failure within a specialized function**.** A "network vulnerability" is a subset of vulnerabilities which can result due to the exploitation of misconfigured systems, insecure network architectures, or trust conditions between nodes within a network. Bug bounties, also known as vulnerability reward programs, are formal programs that allow companies to reward security researchers for responsibly disclosing vulnerabilities within the company’s product, network, or applications, that unaddressed could result in widespread damage to the company and its customers.[5] Vulnerabilities exist in two states: publicly known and previously unknown. Publicly known vulnerabilities are archived through entities such as US-CERT or MITRE’s Common Vulnerability and Exposure (CVE) database.[6] Exploits for these vulnerabilities are housed in locations such as the Offensive Security Exploits Database (exploit-db).[7] Previously unknown vulnerabilities, or “0-day vulnerabilities,” are flaws to which vendors are unaware and no patch exists; the knowledge of 0-days are often close-hold and extremely limited. For simplicity’s sake, the remainder of this paper will use the term "vulnerability" to describe both known and previously unknown vulnerabilities in networks, applications, and designs.

Challenge:

The U.S. Army utilizes a wide array of proprietary and commercial off-the-shelf systems that are integrated across its massive worldwide network that spans numerous classification levels. Most of the Army’s critical systems are underpinned by networked software -- from tanks and missile launchers to battle command and communication systems. The Army does not have one central location for responsibly disclosing software vulnerabilities across all of its systems. Without a means to report vulnerabilities in Army software or networks, vulnerabilities go unreported and leave our information systems exposed to adversarial attacks. As the U.S. Army becomes more and more reliant on technology, it is critically important to understand the growing attack surface

evidenced in Figure 1.

Figure 1. A CVE-Identifier is a number assigned to a specific security vulnerability that is publicly disclosed by security researchers. More than a dozen major security vulnerabilities in significant software products are publicly disclosed on average per day.[8]

Additionally, no US government program exists that permits active security assessments of networks or software solutions using custom tools or techniques. Most importantly, the Army does not have a single entity that tracks discovered issues from initial report through the remediation process to ensure vulnerability resolution in a timely manner. This has led to the current inability for senior leaders to achieve crucial awareness and mitigate risk across the Army IT enterprise.

Due to the complexity of Army IT procurement processes and the fact that software vulnerabilities can be present in everything from major combat platforms (traditionally not understood to contain complex code susceptible to cyber effects) to IT solutions, it is often extremely difficult to remedy vulnerabilities. Personnel who discover vulnerabilities encounter stumbling blocks from the first step of responsible disclosure–initial notification. If an employee does find the contact information for a developer or program office, there is no external incentive or repercussion for a responsible party to action the report or intelligence that is provided to them. Additionally, it is possible that the report recipient could misinterpret the findings, not as valuable and friendly intelligence but rather as a threat to their contract, command, or system. Both scenarios yield the same result–the vulnerability remains and the report is dismissed. This wastes researcher's time, hard work, and promotes a "do-nothing" culture.

The current operating environment for vulnerability researchers within the DoD is an atmosphere fraught with danger and much trepidation. Personnel are hesitant to disclose known vulnerabilities in systems out of a fear of reprisal. Revocation of security clearances, loss of access to IT systems, and punitive action under the Uniform Code of Military Justice are all viable outcomes for someone who casually stumbles upon an interesting finding during everyday work. The most unfortunate outcome is that Servicemembers who become aware of vulnerabilities feel helpless to positively affect the situation. Meanwhile, those who wish to do harm to our Nation are free from such

worries.[9]

The Cyber Warfare domain inherently lends itself to asymmetric warfare; a single actor can unleash devastating effects upon a target or nation-state at will while taking some solace in the fact that they can remain pseudo-anonymous. The notion that it requires a large nation-backed effort to achieve dramatic effects in cyberspace has been continuously debunked since the advent of the hacking collective. For example, in May 1998, seven members of the hacker think-tank "The L0pht" testified before a bipartisan Senate panel about how a single individual could shut the internet down in approximately 30 minutes through attacks to the BGP protocol that allows core internet routers to communicate.[10] More recently the vigilante hacker, The Jester, showed the world how a single individual could successfully wage a war against extremist jihadi groups online, to greater success than many nation-state organizations.[11] Adversaries actively research vulnerabilities within our networks every day; the enemy does not yield to scope or regulations. Finding these gaps in our defenses is a race that we are currently not poised to win because we do not have effective processes in place to leverage Servicemember-derived vulnerability reports. In order to mitigate the next big cyber attack, we must capitalize on and organize our own top-tier talent at the ground level. They should be encouraged and free to utilize their unique skill sets within an environment conducive to conducting research and without fear of punitive action.

High-level solution:

The Army Vulnerability Response Program (AVRP) will be the Army's principle center for all cyber-related issues that impact the Warfighter or cyber security. This includes the discovery of unpatched systems vulnerable to existing exploits or the discovery of entirely new vulnerabilities. Precedent for a vulnerability disclosure program exists in the U.S. Government. The Department of Homeland Security has the "see something, say something" program that enables anyone to report suspicious activity potentially related to terrorism.[12] The U.S. Army utilizes the iSALUTE reporting mechanism to funnel tips about espionage, terrorism, and insider threats to Counterintelligence and Military Police officials for action.[13] Embodying a similar mindset, the AVRP will allow all Department of the Army Civilians and Soldiers to contribute to the safety of digital networks and platforms.

The Army has several programs in place that manage vulnerabilities; however, they do not encompass the tenets of a typical "bug bounty" program. According to Army Regulation 25-2, the existing Information Assurance Vulnerability Management is a top-down program that is focused on the dissemination of security guidance and implementation of system patches.[14] The program

restricts personnel to a subset of approved scanning tools and explicitly denies penetration tests. The Do-It Yourself Vulnerability Assessment Program (DITY VAP) goes a step further by allowing system administrators to scan their networks but continues to deny techniques that include data corruption, data manipulation, data denial, examination of data content, denial of service, or penetration tools. A vulnerability scan is an inadequate technique that cannot reveal the true impact or scope of a gap in the perimeter without a deeper analysis through active penetration testing. These programs are oriented toward network security and do not address specific software systems or combat platforms.

According to a representative within the Army Cyber Operations and Integration Center, there is an existing standard operating procedure (SOP) for vulnerability disclosure but it is not centrally tracked or managed. The current SOP requires an individual who discovers a vulnerability to notify their assigned Information Assurance Manager (IAM) at the local unit level. The IAM, in turn, forwards the report to the installation Network Enterprise Center (NEC) that reports to the Regional Cyber Center (RCC). The RCC forwards the report to ARCYBER, and lastly ARCYBER issues a halt on the utilization of the software application until the vulnerability is addressed.[15] There are no specifics on turn-around time or levels of severity which would trigger the reporting chain. The most concerning aspect of this reporting chain is the lack of awareness regarding its existence; personnel from the IAM level through ARCYBER were unaware of the reporting flow.[16] Lastly, the scope of this report flow is limited to software applications with a certificate of networthiness; vulnerabilities in major end items such as combat platforms would not be reported through this particular mechanism.

It is important to note that alternate outlets for disclosures within Army systems exist outside of the Army. There are enormous international black and grey markets that enable the exchange of 0-day vulnerabilities and exploits. Spanning the ethical spectrum, these markets allow interested parties to buy previously unknown attack vectors from researchers. The lack of legitimate avenues for responsible disclosure findings could cause researchers to feel as though selling their work to exploit brokers is the only way to take advantage of their findings. In the current post-Snowden era, it is also entirely possible that a disenfranchised federal employee could publicly disclose government vulnerabilities through full disclosure websites or public repositories such as GitHub or PasteBin in an effort to have his or her voice heard. Simply stated, the existence and cultural support of the AVRP could mitigate numerous future security breaches and incidents.

The AVRP will serve as the central reporting mechanism for vulnerabilities in Army networks and will receive reports on poor configurations or gaps in security that could allow attackers to degrade

Army systems. These systems include Army digital training management systems, Army Battle Command Systems, logistics procurement systems, and combat platforms deployed in hostile environments. Researchers can report vulnerabilities through a phone hotline or an online submission portal. The AVRP will track all submissions, facilitate the flow of communication with affected entities, and play an integral role in resolving the vulnerability throughout US government networks.

Solution Details:

The AVRP will not be governed solely by a regulation enumerating every detail of its capabilities. Instead, it must rely on agile, creative thinkers that can interpret guidelines in order to harden an array of networks and software applications.

An obvious concern for network defenders regarding the implementation of any sort of bug bounty program is a compromise to the confidentiality, integrity, or availability of production network environments due to bug discovery attempts. The Army can learn from existing industry programs and establish thorough rules of engagement (ROE) that participants must acknowledge and adhere to prior to conducting research. The recommended rules of engagement described below are based on universally accepted tenets of the bug bounty programs from United Airlines, Microsoft, Google, and Facebook. These businesses own products with an enormous magnitude of pervasiveness throughout everyone's daily lives; a vulnerability would have an analogous impact on their product ecosystem as it would for the U.S. Army. The AVRP ROE can be summed up in one phrase: "do no harm." The AVRP is designed for well-intentioned researchers to serve their country utilizing unique skills to harden our defense networks. To accomplish this, researchers must adhere to the following guidelines:

1. The mass collection of personally identifiable information (PII) or sensitive information is prohibited, as is the mishandling of said information. Researchers should make a reasonable effort to minimize the collection of PII or other sensitive information while conducting vulnerability research. Information should be collected only to the extent that it assists in explaining the impact of the vulnerability; researchers should attempt to access solely their own information as applicable. There is no change in the rules concerning the handling of any information garnered during the discovery of a vulnerability, and it will be treated with the same protections as if it were retrieved from Army solutions via conventional means.
2. Researchers may not publicly disclose vulnerabilities found on Army networks and must use the AVRP for reporting vulnerabilities. Vulnerability information regarding Army networks is sensitive and potentially classified information. A researcher discovering a

vulnerability may not disclose this vulnerability to the public or to anyone outside the vulnerability research program, unless provided with specific written authorization after remediation.

3. Researchers may not use automated vulnerability scanners against Army networks. Vulnerability scanners can be dangerous and disruptive to running services. They also create many false positive reports in Intrusion Detection Systems, hindering the work of computer network defense and defensive cyberspace operations entities. While the value of vulnerability scanners is not discredited (their use is encouraged), they should only be employed by assigned personnel with in-depth knowledge of the systems they are targeting and with the right systems in place to quickly resolve any issues vulnerability scanners may cause.
4. Researchers are not permitted to actively or passively interact with third-party entities related to the US government. Interfering with information systems belonging to private entities will subject violators to civilian prosecution.
5. Network-level distributed denial of service attacks are strictly prohibited. Resource and application denials of service are within scope, but must be coordinated prior to testing. The AVRP will provide a test network or environment when possible.

Vulnerability response programs, as they exist today, can be classified into two categories: open and closed. Open programs allow participation by any party, regardless of nationality, legal status, employer, or otherwise. Such a program is inappropriate for a DoD network. Instead, the AVRP will restrict participation in vulnerability remediation to DoD personnel who have applied for and been approved to participate in the program, as outlined below. Inevitably, a concerned citizen will discover a vulnerability through everyday use of Army systems; the AVRP will still receive the report but will not allow the reporter to participate in the remediation process.

A simple web portal will display the program’s ROE while requiring a researcher to digitally sign a commitment to adhere to the aforementioned standards. The failure to comply would result in punitive action against the individual. Upon discovery of a potential vulnerability, the researcher must report the finding(s) to the AVRP through the tracked submission portal. A representative from AVRP will analyze the submission and determine if the report meets a pre-determined severity threshold.

Figure 2. Reporting Flowchart

A key issue faced by vulnerability response programs is the large volume of negligible issues reported by inexperienced researchers. Another common issue is the poor quality of reports that do not properly explain the vulnerability at hand or provide steps to reproduce the issue. The AVRP will clearly define the vulnerability classes the Army is interested in, those the Army is not interested in, and prioritize vulnerability submissions by their potential severity. Following this course of action will encourage researchers to seek out the vulnerabilities with the largest impacts and potentially prevent the program from being overwhelmed by submissions with a negligible security impact. The proposal includes the implementation of a risk matrix that takes into consideration the security impact and threat likelihood with respect to a given vulnerability. Researchers will only submit disclosures that can be defined as a Category 3 vulnerability or higher based on the matrix in Figure 3.

		Security Impact		
		Negligible	Moderate	Severe
Threat Likelihood	Imminent	3	4	5
	Possible	2	3	5
	Rare	1	2	5

Figure 3. Security risk

The security risk matrix is a means to qualify the threat a vulnerability poses utilizing security impact and threat likelihood as the predominant measurements. Exploitation by an adversary is possible within all Army systems and vulnerability impacts to security exist along a spectrum: a negligible risk poses no or limited impact to functionality or capability; a moderate impact causes a degradation in availability or functionality; and a severe impact compromises confidentiality or integrity or results in a complete loss in availability. Threat likelihood accounts for the probability an adversary will exploit a vulnerability. A rare likelihood exists in systems that are not networked or which provide no desirable effects to an adversary. An imminent likelihood indicates a system is certain to be attacked due to its sensitivity, exposure, capability provided to the adversary, or if similar systems have recently been compromised.

The AVRP will provide researchers with a standard submission form that guides the user towards a thorough report. This form will ensure a baseline of information required to understand and reproduce a discovered vulnerability. This key information includes: a concise description of the vulnerability; prerequisites for the vulnerability to exist (hardware or software dependencies); contact information for the appropriate vendor if known; a complete description of steps taken to produce the vulnerability; description (if applicable) of any corresponding known exploits; and space for screenshots or additional report details as needed.

If the report does indeed surpass the defined threshold, the researcher must submit an application to move deeper into the problem area. This application would serve as a “license,” when approved, to conduct a narrowly scoped analysis of an area with close cooperation between the AVRP, the affected vendor or program office, and/or select elements of the Army Cyber Mission Force. The license identification number will serve as the vulnerability tracking ID; metrics included alongside the tracking ID will include date issued, number of days active, severity category, and a log of working group meeting dates. The working groups include the researcher, a representative from AVRP, and the affected vendor or owner as applicable. The goal of these group meetings is to engage all interested parties in an agile manner so that the issue is resolved as quickly as possible. The AVRP will provide licensed researchers with access to development networks that would allow for more precise analysis without a threat to production environments or chance of an adversary intercepting intelligence regarding the vulnerability. The issuance of the research license also protects the researcher from civil, criminal, and/or administrative investigations or charges while operating within the scope of research. Should the reported vulnerability exceed the classification for which the reporter is authorized, the AVRP must keep the reporter notified on progress and updates concerning issue resolution. The AVRP will allow the reporter to apply for an interim security clearance that would expire after the completion of research and remediation on a case-by-case basis.

After receiving application approval and a license identification number, researchers will make every effort to prevent a degradation to production systems and triggering intrusion alerts. The AVRP will act as a liaison between affected organizations and the researcher to determine what is deemed mission critical and help deconflict any issues preventing further research.

Any expertise provided by members of Army Cyber Protection Teams and Cyber Combat Mission Teams could yield extraordinary benefits towards remedying the discovered vulnerability and

improving capabilities of the mission teams. A distinction with a military-focused bug bounty program as compared to similar private sector programs is the direct impact AVRP reports can have on cyber capabilities. While it is clear that the main objective is to remedy all vulnerabilities within Army IT solutions and to share patches with affected partners, a secondary objective becomes readily apparent in that our adversaries will most likely be susceptible to an attack exploiting the same vulnerability. These two objectives are not contradictory; they create a window of opportunity for our cyber forces while also contributing to the health of the security community. The White House, in the wake of the Heartbleed public disclosure, reached a similar conclusion while defending the National Security Agency's claim that it did not know about the vulnerability.[17]

The AVRP will have two roles in reporting vulnerabilities throughout the rest of the US government. Upon initially receiving a report by a researcher, the AVRP will issue an unclassified alert to all government entities. After successful resolution, the AVRP will facilitate the dissemination of patches throughout the USG; after classification review, the AVRP will facilitate the release of the patch to the public.

All Servicemembers swore an oath to support and defend the Constitution of the United States against all enemies, foreign and domestic. Service members would participate in the AVRP without any need of additional incentive -- using their skills to serve their country would be sufficient. In an attempt to remain competitive with the private sector, the AVRP can leverage existing incentives programs within the Army to encourage participation without providing the direct monetary rewards that other bug bounty programs offer. The security risk matrix in Figure 3 inherently lends itself to the development of a program leaderboard. Participants will gain points based on the severity and impact of their disclosure, ranging from three to five points. The Army could host an annual competition with the leaderboard publicly available. At the conclusion of each iteration, the Army could induct the top contributors into the AVRP "Hall of Fame" while offering them their choice of select incentives. In an informal study with several Army Cyber Officers, the top requested incentives were as follows in order by priority: a guaranteed slot in the Advanced Civil Schooling program for graduate studies; training with industry opportunities with businesses such as Google or Microsoft; participation in security conferences such as DEFCON, Black Hat, and ShmooCon; follow-on assignment of choice; branch transfer into the cyber career field; and lastly the opportunity to take additional training courses through private vendors. One security researcher stated, "I would bring the Army to its knees for DEFCON TDY," an exaggeration highlighting the overlap in known, undisclosed vulnerabilities and the excitement for this type of program.[18]

Enterprise benefits:

Before truly enumerating the benefits of implementing the Army Vulnerability Response Program, we must establish a baseline assumption upfront: any degradation to confidentiality, integrity, or availability that might result from participants' research can be caused by our adversaries. With that in mind, we can begin to appreciate the numerous benefits of the program.

Foremost, the AVRP is a conduit to free intelligence. AVRP reports provide senior leaders visibility on previously unknown risks within our combat and support systems. These reports can be included in Commander's Update Briefs and will allow decision makers to array their forces in support of the highest priority missions and threats, while improving the command's understanding and management of risk.

The AVRP is a cost-effective means to increase the security of our software-dependent systems. Often Servicemembers stumble across vulnerabilities during the countless hours they spend interacting with their systems. With the AVRP, Servicemembers who maintain and operate systems, and in many cases become experts in their deployment and utilization, now have a conduit through which to funnel their vulnerability reports. Similar engineering efforts to identify the same vulnerabilities are complex and time-consuming. By enabling AVRP, only a small group of experts is required to validate reports, gaining significant efficiencies for the enterprise. Since it is not possible to assemble engineering efforts to continuously assess the security of every networked Army system and combat platform, AVRP is the next best option to effectively and dramatically increasing the number of eyes on the problem at no cost.

A subset of the cyber workforce is passionate about their profession and maintains personal projects aligned with cyber security, in addition to their regular duties within the Army, which may or may not be associated at all with cyber security. The AVRP would provide these hobbyists with a constructive outlet that would harness their personal time while allowing the employee to directly contribute to the safety of our Nation.

Through the AVRP leaderboard, Army Cyber will gain greater visibility on talent within the workforce. From seasoned researchers that serve within combat arms to newly minted lieutenants within the cyber branch, the AVRP can help identify technically gifted personnel and offer them new opportunities to serve. Providing these creative minds with freedom of maneuver will inevitably enable job satisfaction and increase the retention levels of our most gifted personnel.

As a closed-disclosure program, AVRP allows DoD members to conduct assessments which reduces the risk of exposure to additional threats and spillage that might result from recruiting outside organizations to conduct third-party security audits. Including all Soldiers and Army Civilians within the program crowdsources our security concerns and allows DoD Red Teams and Cyber Protection Teams to focus on the most critical priorities.

Finally, by enacting AVRP, the Army can demonstrate to the public and Congress the maturity and capability of its workforce without the need to outsource talent from the private sector. This encourages retention and reinforces the cyber force's standing as a true profession. Throughout the security industry, experts view corporations with standing bug bounties as more mature entities who are capable of recognizing that security vulnerabilities are inevitable. Further, bug bounty programs signal that the organization is receptive to advice in pursuit of continuously improving its security posture.[19]

Policing practices, networks, and policies with security as a forethought is a clear sign that we are members of a profession. Giving the Army the ability to share discovered vulnerabilities with the private sector would help mend damaged relationships and assist with regaining public trust.[20] Fundamentally, the AVRP is aligned with the Army Values and service objectives.

Future Work:

While certain aspects of the AVRP can be implemented immediately, the Army must change some current policies to improve the program's impact. One area of concern is the lack of control and/or visibility of source code for contracted solutions. It is recommend that all procurement projects that involve the development of source code have their code hosted on DoD-maintained version control servers. This would provide a new, improved level of visibility, allowing auditors the opportunity to evaluate developers' methods for secure coding and would allow security testers to make specific recommendations to fixing vulnerabilities through white box testing. Additionally, it accelerates response efforts because it eliminates the coordination required to gain access to source code developed and maintained by a myriad of contractors.

Tangentially, it is recommend that contracts include clauses that require developers to remedy

vulnerable code within a fixed timeline throughout the lifespan of the software's use. Placing the onus of secure code onto the developer will undoubtedly improve the security posture of our networks and cause a foundational shift towards a security-first mentally when developing software for the DoD.

In the future, all providers of Army services must provide a duplicate test environment of their service for the purpose of enduring vulnerability testing by the Army's cyber experts. This service should be populated with fictitious data, minimizing potential exposure to PII or other sensitive information should a vulnerability be discovered. Furthermore, should a researcher accidentally disrupt or modify a service, risk to operational Army services would be minimized.

The AVRP must extend the protection provided under the Whistleblower Protection Act of 1989 or provide a new framework to protect well-intentioned researchers from punitive actions.[21] Congress enacted the Protection Act to ensure any whistleblower who reported agency misconduct through proper channels was protected from reprisal. Participation in the AVRP would cease immediately if a researcher, operating within the published ROE and scope of the program, was negatively impacted. The extended protection must also allow the researcher to publicly disclose the vulnerability if the AVRP is unable to resolve the issue within a fixed time window of 120 days.[22] For the AVRP to be truly successful, the Army must wholly adopt a culture conducive to securing our networks through a crowd-sourced methodology. The security of our networks impacts every Servicemember and we can improve if we protect those who volunteer to help.

If implementing an Army-run bug bounty program is not within the immediate goals/desire of any organization, there are third-party programs that can manage the program for the Army such as the Zero Day Initiative (ZDI) and Bug Crowd. Utilization of these third party programs would require a change to their current practices to handle classified disclosures which would most likely come at a substantial cost.

Summary:

In a speech during the Joint Service Academy Cyber Security Summit at West Point, NY on May 14, 2015, ADM James Winnefeld Jr., the Vice Chairman of the Joint Chiefs of Staff, stated we must "...render the term attack irrelevant by configuring our networks and the software running on them in ways that make them impossible to attack in the first place… we all win if our networks are more

secure."[23] The Army Vulnerability Response Program is one essential step along the road to accomplishing this seemingly impossible feat. The U.S. Army has the means, personnel, and urgent need to implement this program now and we must do so to ensure the safety of our Warfighters, our critical systems, and sensitive information.

The views presented throughout this paper belong to the authors and do not represent the views of the US Government, the U.S. Army, or the Madison Policy Forum.

About the Authors

Captain Rock Stevens began working in IT as a network administrator at the age of 15. He served as a Company Commander within the Army's 780th Military Intelligence Brigade (Cyber) and was selected as a 2015 Madison Policy Forum Military-Business Cybersecurity Fellow. He is currently pursuing a master's degree in Computer Science at the University of Maryland College Park.

Captain Michael Weigand has been a student of the cyber security world since his college professors found out about his GPS guided model truck. He has interned or briefly worked for iRobot, USC Institute for Creative Technologies, and DARPA. After spending his lieutenant years in the Infantry, he recently joined the newly formed Army Cyber Branch and is stationed at Fort Meade, Maryland.

Footnotes

[1] Sanger, David, and Nicole Perlroth. "White House Takes Cybersecurity Pitch to Silicon Valley." The New York Times. April 26, 2015. Accessed August 5, 2015. http://www.nytimes.com/2015/04/27/us/white-house-takes-cybersecurity-pitch-to-silicon-valley.html?_r=2.

[2] Schmidt, Michael, and David Sanger. "Russian Hackers Read Obama's Unclassified Emails, Officials Say." The New York Times. April 25, 2015. Accessed August 5, 2015. http://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html?ref=us&_r=1.

[3] Crawford, Jamie. "Carter: Russians Hacked Pentagon Network." CNN. June 4, 2015. Accessed August 5, 2015. http://www.cnn.com/2015/04/23/politics/russian-hackers-pentagon-network/.

[4] Nakashima, Ellen. "With a Series of Major Hacks, China Builds a Database on Americans." Washington Post. June 5, 2015. Accessed August 5, 2015. https://goo.gl/rjQQfv.

[5] Solomon, Sharon. "11 Essential Bug Bounty Programs of 2015." The State of Security. February

10, 2015. Accessed August 5, 2015. http://www.tripwire.com/state-of-security/vulnerability-management/11-essential-bug-bounty-programs-of-2015/.

[6] "Common Vulnerabilities and Exposures." CVE. Accessed August 5, 2015. https://cve.mitre.org/.

[7] "Offensive Security Exploit Database Archive." Exploits Database by Offensive Security. Accessed August 12, 2015. https://www.exploit-db.com/.

[8] Cleaned data from CVE List, Master Copy, http://cve.mitre.org/cve/cve.html.

[9] Cox, John. "Should the U.S. Allow Companies to 'hack Back' against Foreign Cyber Spies?" Washington Post. May 23, 2013. Accessed October 22, 2015. https://www.washingtonpost.com/news/worldviews/wp/2013/05/23/should-the-u-s-allow-companies-to-hack-back-against-foreign-cyber-spies/.

[10] Net of Insecurity. The Washington Post. Accessed August 12, 2015. http://www.washingtonpost.com/sf/business/2015/06/22/net-of-insecurity-part-3/.

[11]http://www.sans.org/reading-room/whitepapers/attacking/jester-dynamic-lesson-asymmetric-unmanaged-cyber-warfare-33889

[12] "If You See Something, Say Something." Department of Homeland Security. Accessed August 12, 2015. http://www.dhs.gov/see-something-say-something.

[13] "iSALUTE - Suspicious Activity Reporting." U.S. Army INSCOM. Accessed August 12, 2015. https://www.inscom.army.mil/isalute/.

[14] U.S. Department of the Army. Information Assurance. Army Regulation 25-2. Washington, DC: U.S. Department of the Army, March 23, 2009.

[15] Capt. Jim McColl in discussion with the authors, August 2015.

[16] 'Cyber Security Researcher Central Reporting Hotline / "Bug Bounty."' Department of Defense milSuite. June 16, 2015. https://www.milsuite.mil/book/ideas/3762

[17] Daniels, Michael. "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities." The White House. April 28, 2014. Accessed August 12, 2015. https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

[18] Capt. Alexander Eubanks (cyber security researcher) in an interview with the authors, August 2015.

[19] Kerner, Sean Michael. "Building Security in Maturity Model Includes Bug-Bounty Programs." Building Security in Maturity Model Includes Bug-Bounty Programs. October 30, 2013. Accessed October 22, 2015. http://www.eweek.com/security/building-security-in-maturity-model-includes-bug-bounty-programs.html.

[20] Desiderio, Andrew. "Poll: Few Trust NSA Data Collection Practices." RealClearPolitics. May 20, 2015. Accessed August 12, 2015. http://www.realclearpolitics.com/articles/2015/05/20/poll_few_trust_nsa_data_collection_practices_126662.html.

[21] "Information on Whistleblower Protection Act and Whistleblower Protection Enhancement Act." US Government. Accessed August 12, 2015. https://www.sec.gov/eeoinfo/whistleblowers.htm.

[22] "Feedback and Data-driven Updates to Google's Disclosure Policy." Project Zero. February 13, 2015. Accessed October 22, 2015. http://googleprojectzero.blogspot.jp/2015/02/feedback-and-data-driven-updates-to.html.

[23] "ADM James A. Winnefeld," YouTube video, 20:50, posted by "Army Cyber Institute," June 16, 2015, https://www.youtube.com/watch?v=j9cFHYHMQcY&list=PLtUuPz3a0Gz-exkdE3tnpxLaIeBWZkucY&index=7