Response to Written Questions Submitted by Honorable Jerry Moran to Mårten Mickos

*Question 1.* What separates a good faith researcher from a malicious actor? What's to stop a criminal from posing as a researcher? How can companies or vendors tell the difference?

Response. Intent is what separates a good faith security researcher from a malicious actor. Researchers that are reporting vulnerabilities through lawful channels are doing so with the intent that the vulnerability report be delivered to the owner of the system for the bug to be resolved.

Vulnerability disclosure and bug bounty programs are so designed that they provide no particular benefit or special access to the participants. On the contrary, the programs generate additional work for the participant while collecting various pieces of information about them. For these reasons, a malicious actor has something to lose and nothing to gain in such a program. It is more rational for the malicious actor to engage in their unauthorized activity outside of the program.

Like in most professional endeavors, it is at least in theory possible for a criminal to pose as a legitimate participant. But given that there are no benefits but only obligations in a program, this would not be rational behavior. The only way to receive a benefit from a vulnerability disclosure or bug bounty program is by reporting a valid vulnerability to the owner of the system. When that happens, a vulnerability can be removed and rendered unusable by criminals.

Criminals, for the above mentioned reasons, do not wait for vulnerability disclosure or bug bounty programs to start, and they obtain no benefit from joining such programs if they exist. Criminals engage in their unauthorized activity at any time and outside any formal program.

When researchers bring security vulnerabilities to the attention of companies and organizations, they should assume good faith until proven otherwise.

The question of whether an entity operating a program can tell the difference between a well-intended researcher and a criminal becomes philosophical or even irrelevant. Outside of the program, any criminal activity is possible and often likely. Inside the program, only good and non-criminal deeds are rewarded.

The above text describes the general case. Additionally, there can be a special case of a bug bounty program in which the program-operating entity indeed does offer special access or benefits to the participants. For instance, a company may provide test accounts or other credentials to participating researchers so that they may venture deeper into the computer system in their hunt for vulnerabilities to report and be rewarded for. In such programs, the participating researchers go through additional vetting and screening. The exact nature of the screening depends on the company's or organization's preferences and may include verification of identity and tax ID, verification of home address, criminal background check, and so on. With these additional screening requirements, the operator of the bug bounty program guards itself against malicious actors gaining access to the program in question.

For an overview of the motivations of ethical hackers and for personal profiles of a number of them, we recommend reading the 2018 Hacker Report that is available from HackerOne, Inc., on our website www.hackerone.com and by contacting us by email at info@hackerone.com.

*Question 2.* What is the role of bug bounty programs when faced with extortion attempts?

Response. Extortion has absolutely no role in bug bounty programs.

Whenever a situation develops that may indicate an extortion attempt, HackerOne advises the sponsor of the program (its customer) to notify and work with law enforcement for guidance and instructions. It is always the entity with the bug bounty (or vulnerability coordination) program that determines whether conduct by a hacker or hackers is authorized or unauthorized. Bug bounty platform providers such as HackerOne act as a preventative service.

There are situations where immature researchers may ask for a bounty in an impolite or even threatening way. Often, such situations can be de-escalated with the help of mediation and diplomacy. Hackers do commonly suggest or ask for specific bounty amounts from the vendor.

The size of the bounty is largely determined by the severity of the vulnerability, and severity can be properly assessed only by the customer. So the finder is in a position of no control at all over the payment outcome. To balance this, they often make suggestions, requests and claims for specific bounties in the hope that the customer will be open to suggestions. As many hackers are young and all of them are impatient, the language of such requests may not seem proper to someone not familiar with the trade, even though the hacker has the best of intentions.

*Question 3.* According to your testimony, the diversity and scale of the hacker community allows the "hacker-powered security" model to identify vulnerabilities that automated scanners and permanent penetration testing teams will not. Can you please further explain this sentiment? Are there any metrics or numbers that are able to cite to quantify the effectiveness of the model over other approaches?

Response. Customers on HackerOne have resolved more than 65,000 unique security vulnerabilities to date by working with the hacker community. A good portion of these customers have reported back to HackerOne that they are finding vulnerabilities that they could not otherwise detect with scanners or penetration testing (also called pentesting). The strongest metric in support of hacker-powered security is the fact that even after deploying scanners and pentests there are innumerable security vulnerabilities that bug bounty and vulnerability disclosure programs identify.

There are a number of reasons for this. A key reason is that scanners and penetration testing are limited in scope whereas hacker-powered security is broad and diverse.

A scanner has been programmed by engineers to detect specific previously known vulnerability types, but it is limited in its ability to modify its search or "think outside the box." Though useful, scanners cannot find what humans can. Penetration tests are conducted by humans and therefore represent more intellectual variety and creativity than scanners. But they cannot measure up against a broad and creative collection of external researchers. Penetration tests

follow pre-defined guidelines and are designed to test for a specific set of vulnerabilities. Often, customers are more eager to get a clean report than to find all possible vulnerabilities.

In both the case of scanners and of penetration testing, the customer is paying a fixed price for effort. But in the case of hacker-powered security, the customer pays for result. Hackers do not get paid unless they find something of value to the customer. This leads the hackers to try harder and think more creatively, and that in turn leads to superior results.

*Question 4.* Your testimony described vulnerability disclosure programs with the motto of "If you see something, say something," and further elaborates how the outside hacker will be invited to disclose the vulnerability to the system's owner. During the disclosure process, is it a common practice for the hacker to actually take exposed data in order to demonstrate proof of vulnerability to the company? If so, is there a standard type or amount of data that these [sic] is needed for the hacker to demonstrate authenticity?

Response. The amount of evidence that it is prudent to collect when discovering a security vulnerability is a topic of great interest to the security community. On the one hand, the hacker is bound and committed by the program rules not to cause harm or obtain any data that is not needed for the work. On the other hand, there are situations where perhaps the only way of demonstrating that a breach could be possible is to actually exfiltrate some data.

Entities that operate bug bounty programs declare on their program page the rules for the hackers. Typically, they will prohibit data exfiltration, as this example from a prominent bug bounty program shows: "Findings not eligible for bounty: ... Internal pivoting, scanning, exploiting, or exfiltrating data from internal [company name] systems."

It should be noted that a hacker may not initially know what is inside a data file found. In order to determine the nature of the file, the hacker may have to open it, which for practical purposes may mean downloading it, which amounts to exfiltration. If the contents are irrelevant, then no harm was done. If the file contains pointers to other data sources, or perhaps credentials to another system, then this is valuable information for resolving the security problem. But if the contents turn out to be customer or personal information, then the hacker must immediately erase any such copies of the file and refrain from opening it or using it again. The determination of whether it is permissible to open the file or not can be made only after the file has been opened.

*Question 5.* HackerOne's 2018 Hacker Report and a 2016 study conducted by the National Telecommunications and Information Administration (NTIA) both indicated that profit is a relatively limited motivation among hackers participating in coordinated vulnerability disclosure programs. Given the panel's experience with professionals in this field, could you please further describe the predominant motivators?

Response. In the course of its business, HackerOne has enabled tens of thousands of hackers to find and help fix over 65,000 security vulnerabilities. The motivations behind the hackers' work are as diverse as the group. In the hacker surveys we have conducted, we consistently see hackers operating under multiple motivations.

Financial rewards are essential and important, but they are far from the only motivation. The presence and success of numerous vulnerability disclosure programs (i.e., programs that pay no financial rewards) serve as a clear indicator that there are plenty of hackers ready to hunt for security vulnerabilities for other than pecuniary reasons. For instance, in the various programs by the Department of Defense, about 3,000 vulnerabilities have been reported into the vulnerability disclosure program and 600 within the bug bounty programs.

Many hackers hack for the intellectual challenge. They want to learn more and they are eager to know that they have the skill to find a hole in the armor of a famous company or government entity. Being thanked or acknowledged by a prestigious vulnerability disclosure program is a great motivation.

Often, hackers hack in order to find like-minded people and be able to collaborate with them. It is a reward in itself to be able to interact with someone with unusual skill or intellect.

Others hack for the pragmatic reason of advancing their careers. The list of vulnerabilities found that each hacker has on their individual HackerOne page serves as evidence of their skills. It helps them gain entry to colleges and universities or to land a security job at a company or other organization.

For many, there is an altruistic motive in hacking. They want to make the world a more secure place. They want to contribute to society. They have a sense of duty and feel that if they know how to detect vulnerabilities, it is their mandate to report them to the owners of the various systems.

*Question 6.* Would you agree that it is absolutely critical for companies to administer any vulnerability disclosure program responsibly based on sound principles (such as those included in DOJ's 2017 guidelines) as it has obvious impacts on industry-wide use of these types of programs that are proven to protect consumers?

Response. Yes, HackerOne applauded the U.S. Department of Justice for its 2017 guidelines for vulnerability disclosure programs (VDP). The DoJ's guidance reflects best-practices across the industry and is a critical document for any organization. Indeed, in many ways, HackerOne is dedicated to facilitating the responsible implementation of VDPs across the broad spectrum of vulnerable entities in line with the DoJ's guidance.

*Question 7.* Given the unique national security aspects of working with DOD, I am interested to hear more about HackerOne's involvement in the vulnerability disclosure programs aiding our Armed Services, starting with the "Hack the Pentagon" program and followed by the "Hack the Army" and "Hack the Air Force 1.0 and 2.0."

Response. The Department of Defense's Defense Digital Services pioneered the first ever Federal bug bounty challenge, "Hack the Pentagon," in 2016. The DoD is continuing to do so by engaging with the global hacker community through its ongoing vulnerability disclosure policy.

Since the Hack the Pentagon program launched in 2016, over 3,600 vulnerabilities have been resolved in government systems through the bug bounty and vulnerability disclosure challenges

on HackerOne. Working with the ethical hacker community supplements the useful work the DoD's internal security teams are already doing.

Hack the Army

The Hack the Army Bug Bounty program ran from Wednesday, November 30, 2016 to Wednesday, December 21, 2016. Hackers reported more than 118 valid unique security issues.

Through this program, the Army was able to tap into the reservoir of diverse hackers on HackerOne, many of whom would otherwise not work with the Army, augment the work the Army red teams are already doing to help secure their systems and networks, and increase the security of mission critical systems and networks that house information critical to military recruiting.

The Army chose as its target digital assets that might have been used as a stepping stone for reaching personally identifying information about Army recruits - colloquially referred to as "the crown jewels." Ensuring this data was secure was a high priority for DoD because of the sensitivity of the information for America's potential war fighters.

The most significant vulnerability found was due to a series of chained vulnerabilities. A researcher could move from a public-facing website, goarmy.com, and get to an internal DoD website that requires special credentials to access. The researchers got there through an open proxy, meaning the routing was not shut down the way it should have been. The researcher, without even knowing it, was able to get to this internal network because there was a vulnerability with the proxy and with the actual system. On its own, neither vulnerability is particularly interesting. Paired together, they become critical.

Automated testing tools are not capable of such leaps of logic. It requires a highly skilled and creative researcher (or team of researchers) to chain together a number of independent flaws in order to create a path to the critical inside of the system.

The Army remediation team that owns and operates the websites, as well as the Army Cyber Protection Brigade, acted quickly. Once the report was submitted, they were able to block any further attacks, and ensure there was no way to exploit this chain of vulnerabilities.

Hack the Air Force

The Hack the Air Force Bug Bounty program ran from May 30, 2017 to June 23, 2017, with nearly 300 individual hackers participating in the bug bounty challenge. More than 50 hackers earned bounties for reporting more than 207 valid unique security vulnerabilities, the first of which was reported in less than a minute from the start of the program.

Some of the vulnerability reports received an initial response time of less than a minute by the Air Force security teams. The average time to resolution during the challenge was 4 days. What this means is that the Air Force's security team was extremely fast at processing reports, verifying them and resolving bugs, making the systems more secure faster.

Hack the Air Force 2.0

On December 9, 2017, the first day of the challenge, 24 hackers met in New York City and participated in a live hacking event -- the first ever to include federal government participation on- site. DoD and U.S. Air Force personnel worked alongside the vetted and pre-selected hackers to simultaneously report security flaws and remediate them in real-time. Together, they collaborated to find 55 of the 106 total vulnerabilities during this nine-hour hacking event.

Twenty-seven trusted hackers successfully participated in the Hack the Air Force bug bounty challenge — reporting 106 valid vulnerabilities and earning a total of $103,883. Hackers from the U.S., Canada, United Kingdom, Sweden, Netherlands, Belgium and Latvia participated in the challenge. In this event, the highest single bounty of any Federal program -- $12,500 -- was awarded.

*Question 8.* More specifically, were there lessons learned from the earlier programs that your company addressed and implemented in the more recent programs?

Response. Working with its DoD counterparts, HackerOne and the security research community continue to improve its programs. We regularly revise and improve our internal process descriptions and our external program guidelines in order to reduce the risk of failure in a program and to increase the overall productivity and effectiveness of hacker-powered security. We also continually learn more about the digital assets of our customers so that we can provide better advice on which assets to include in a program, and at what phase of the program.

As our customers develop a thorough expertise in operating a bug bounty program, we may recommend events where hackers and the security team of the customer are brought together for a live hacking event. We did so during “Hack the Air Force 2.0” and the results exceeded expectations.

Hack the Air Force targeted operationally significant websites and online services. The goal of the program was to explore new approaches to its security, and to adopt the best practices used by the most successful and secure software companies in the world. The preliminary results indicate nearly doubling the results of the first Hack the Pentagon program a year earlier.

With every DoD bug bounty the pool of invited participants has grown, with the intent of opening it wider to continue to include all qualified participants. By now, every person on HackerOne is legally permitted to participate in the DoD’s vulnerability disclosure program (VDP). To date, the DoD’s VDP has resolved more than 3,000 security vulnerabilities.

*Question 9.* How did your company account for the specific capabilities and functions of the different services your company worked with?

Response. The key to success in a bug bounty or vulnerability disclosure program lies in diversity of approach and specificity of skill among the hackers. That is why HackerOne has established the world’s largest community of security researchers, also known as white hat hackers. By having an enormous pool to draw from, we ensure that for each particular program there is a large enough group of hackers with the particular skills needed. We record and keep track of skill profiles in our hacker database. When a new program launches, we can find the hackers most likely to have the required skills.

As new customers launch programs on HackerOne, a useful cross-pollination of skills often happens. The new customer typically brings along hackers with deep skills in their particular digital asset. These hackers can then find other programs with similar profiles. And from those other programs, existing hackers may engage in the new program. In this way, over time, individual hacker skills are strengthened, and the overall skill profiles in the HackerOne community become more complete.

Additionally, both HackerOne and its clients may arrange for additional education, training and briefing of hackers in specific areas of technology. The more information there is available, the sharper the skills and the better the results of bug bounty programs.

Arguably the best source of learning for ethical hackers is the Hacktivity feed () where vulnerability reports are being published by various companies and government agencies for others to learn from once the vulnerability has been fixed and removed.

*Question 10.* Please explain the utility of a combined pool of federal employee and outside participants.

Response. The success of cyber security is measured not by how many good events there are but by how many bad events can be avoided. The best results are achieved by multiple layers of security. Even if one layer occasionally fails, there is another layer that will catch the deviation from the norm.

Cyber security starts with the design of the digital system. This is the first layer of security. Later in the software lifecycle comes quality assurance, which also removes weaknesses. When a digital asset is ready for production use, it still needs testing and validation. This is where internal and external bug hunting teams come into the picture. Internal teams of employees have the benefit of inside knowledge of the system. External teams of hackers have the benefit of lack of bias. These and other, more technical, layers of security are needed for the best outcome.

A theme we heard over and over again while working with the DoD is that military and civilian personnel need hands-on training whenever possible. This keeps their skills sharp and allows them opportunities to see unique tactics from a highly skilled researcher community. Allowing employees to participate in bug bounty programs provides realistic training experiences in a controlled environment, at a low cost.

*Question 11.* Your testimony states that $250,000 is the current maximum bounty listed across all programs that the company administers for its clients. Are the maximum bounty amounts pre-determined in agreements with your client companies?

Response. On HackerOne's platform, it is the customer that sets the bounty criteria, often based on a recommendation from HackerOne. HackerOne maintains a set of recommended bounty amounts that we derive from historical bounty payment data, adjusting for size and ambition level of the program in question. The bounty amount is typically a function of the severity of the vulnerability and the value of the digital asset in which the vulnerability was found.

The client company has the full right to deviate from their own criteria and pay out higher bounties than advertised. As a matter of fact, many programs do not publish or advertise any maximum bounty.

In addition to bounties, customers can choose to pay individual bonuses to hackers. For instance, if a hacker has prepared an unusually well-researched and well-written vulnerability report to the customer, the entity may choose to reward the hacker with a bonus on top of the bounty. The bonus amounts are typically small. In 2017, less than 5% of all hacker rewards were bonuses.

*Question 12.* Your testimony stated that the Computer Fraud and Abuse Act is in need of modernization to prevent liability of hackers acting in good faith in identifying vulnerabilities to protect consumers. Do you have any specific recommendations related to modernizing the law?

Response. Current law, particularly the Computer Fraud and Abuse Act (CFAA), does a disservice to the internet and its citizens. Congress should amend it to reflect the modern-day needs of the country's cybersecurity community, including the value and necessity of voluntary disclosure programs.

The CFAA fails to define the terms "without authorization" or "exceeding authorized access," which are key elements of the law. This broad undefined language has resulted in the CFAA being called one of the most controversial, confusing, and inconsistently interpreted laws in the country. We suggest that the law should clarify "without authorization" and distinguish between bad intent on the one hand, and good intent or innocent lack of intent on the other.

While intended as a criminal law preventing malicious hacking, a 1994 amendment to the bill allows for civil actions. We suggest that the CFAA focus on criminal liability rather than civil liability. Much of the chilling effect created by the law originates from its broad interpretation in civil cases, where the burden of proof is reduced.

HackerOne also suggests that violations of contractual obligations, such as a website's terms of service, must not form a basis for criminal charges. Further, it should be clarified in the law that if access to data is already authorized, gaining that access in a novel or automated way is not a crime (i.e., changing IP addresses, MAC addresses, or browser User Agent headers). Finally, minor violations of the CFAA should be punishable with minor penalties, ensuring the punishment fits the violation.

HackerOne urges Congress to modernize the CFAA and related laws to reflect the necessity to fight cybercrime with modern-day tools and processes, including particularly voluntary disclosure programs.