# ‘Drive It Like You Stole It’: When Bug Bounties Went Boom, Part Three

Sep 1, 2021 **By** Dennis Fisher

*After more than a decade of evolution and innovation, bug bounty programs had proven to be invaluable tools for organizations in many industries to help improve their security with the help of outsiders. During Barack Obama's second term, some administration officials began looking at bounties as a potential way to jump-start the effort to upgrade federal government's security programs. The idea was a radical one, given the government's institutional resistance to change, not to mention the inherent risks of allowing outside hackers to look for bugs in target sites. So they decided to start slowly. By hacking the Pentagon.*

*Note: All job titles and positions reflect the person's role at the time of the events.*

*Read part one and part two.*

Alex Romero (CISO of the Defense Media Activity): I tried to recreate the potential of the crowd to come after hard assets, because I tried literally every tool that I could find, every open source tool that I could get my hands on to hack myself. So I actually tried, I think, seven months before we officially did the whole Hack the Pentagon thing. The Defense Digital Service wasn't really formed yet, but I reached out to my lawyers and asked, "Can we use this bug bounty thing? It seems like a good idea." And they're like, "Oh, hell no. Horrible idea." Like, "You're not going to invite hackers to come test our sites." So, how can you get after that problem? Well, I mean, thinking like a hacker. When I was in the Marines, we fought and trained like our adversaries did. But we weren't doing the same thing for our networks. So, that always stuck with me. We could do better. We have to do better.

So I met Chris Lynch, met Reina Staley, Corey Harrison. Those were the tri-founders of DDS. Then from that point on, once we realized, "Okay, this is a good idea. How do we get everybody on board? Who are all the stakeholders?" That was really one of the hardest parts. Yes, I might own the systems, but the network on DoD is owned by many. And what other issues could there be? We had done all sorts of pen tests and red teams, because we didn't want to get embarrassed by anything that the researchers found. We thought we were pretty good, but it turns out we weren't.

Katie Moussouris (Chief Policy Officer, HackerOne): I was giving a guest lecture at a joint symposium that was Harvard Kennedy School and MIT Sloan School. So, first of all, it was a career highlight for me because I stayed in the Charles Hotel nearby. And that was actually a hotel that I used to use to clean myself up as a homeless teenager. At the lecture, I was spotted by Michael Sulmeyer (director for plans and operations for cyber policy in the Defense Department) and he is now serving in a cyber position somewhere in the White House. And he was sitting in on that lecture and he said, "Have you ever been to the Pentagon?" And I was like, "No," and he said, "Well, would you come brief the Pentagon if I invited you?" and I said, "Of course I would."

And I briefed an audience of various people that Michael pulled together and among them was Lisa Wiswell and she ended up taking over his position when he moved into a different role. So I showed Lisa and Charley Snyder, who also was in a policy role in the Pentagon, around ShmooCon a little bit. And then we talked on and off, beginning at that point for years. So it was conversations over several years where anytime I was in town in DC, I would stop over at the Pentagon for a visit and talk to them more, answer their questions about scope, scale, and preparation. Once she called and said, "Defense Digital Service launched, we want to pursue a bug bounty as one of the first big major public things that we do." I was like, "All right, well, let's just make it so that you don't wreck yourself." So what Lisa's ideas were, and I'm sure that RoRo had some of these as well, but Lisa was the one who basically rallied all of the different branches of our military that have offense capabilities. So she basically was like, "You know what? Katie says that we should test our stuff first. Why don't we do it with all the various cyber commands across the military?" And so there was a lot of bureaucracy hacking that she did.

Alex Romero: So fast forwarding past that moment in time to when we actually were told to make it happen, because now these folks were essentially operating on behalf of the Secretary of Defense, and that comes with all sorts of additional authorities. If the SecDef says to do it, then you get it done. Yeah, so the conversations are difficult, and actually that's where Katie was in a few of those conversations. We actually used some of her reference videos when we were trying to educate people on what a bug bounty was. And then she shows up to one of the conversations. I don't remember what color her hair was at the time, but definitely not fitting in either. She came ready, I'll put it that way, to have that discussion. But I think a lot of the work had already been done by the team to prep the battlefield, if you will.

I would put a lot of this and a lot of the success on Lisa Wiswell, and Charley. They did the bureaucracy hacking that allowed us to get to the point where we could actually run the challenge. Once we actually kicked off the challenge, the ball was in my court in terms of making sure it was a success. Because the untold story was, a lot of my leadership was not happy with this. They basically were like, "Well, participate, but it doesn't necessarily need to be a success." I was not of the same opinion. So I reached out to Chris Lynch at the time and I was like, "Well, I personally think this is a valuable tool, and I would like it to be a success." So there were various folks, not to put anybody down, but they were afraid of what could happen if we just invite researchers to come hack on our stuff, and they can pivot and find other ways in. But that's exactly what you want them to do. So, it's a completely different way of thinking.

> ***"Hey, we're going to hack your shit. For real, we are. Here's the memo that says so."***

Katie Moussouris, left, and Lisa Wiswell Coe.

Lisa Wiswell Coe (program manager, Hack the Pentagon): Really, if the first people you're talking to aren't the lawyers, then you've got a problem because at the end of the day, all this is, is a legal mechanism where a legal mechanism doesn't exist at present. It's essentially hacking a law or a suite of laws in order to find a loophole to allow people to do something, to give them authorization to do something that is otherwise a felony. I think in the first several sets of not just the Vulnerability Disclosure Policy discussions that were happening in the public space, but also specific to the assets that were selected for some of the initial bug bounties, you can see that it was intentional to try to make sure that the things that citizens rely on, not just me as a policy person in DoD, but the things that the world relies upon are the things that we're taking very seriously. And yet, the implication might be that they're not secure now. But, the ground truth is we're not, and it's no longer something we're going to disguise from you. We're not going to keep our heads in the sand any longer.

Alex Rice: That initial project was pretty successful for where they were at. Not just in terms of the assessment itself, but in convincing folks that the department submission could benefit from hackers on the outside attributing to it in a meaningful way. One other note that's worth touching on with this is that in that process the team did not have a vulnerability disclosure program at the time. And the momentum internally to establish a VDP wasn't there. So as part of our proposal to them to run their proof of concept we added the ability for them to host a VDP program at the same time to make it as easy as possible for them to have a VDP program set up to handle that ongoing relationship. And what if somebody finds something outside of the challenge? What do we do with it? We could run this narrowly scoped by bounty proof of concept, but what if somebody finds something that's in a different system? What do we do with it? So we were kind of 11th hour successful at making the case for a VDP program to get spun up as an add-on to the Hack the Pentagon program. So it was originally just a bug bounty proof of concepts, ended up being a bug bounty proof of concept, which you get its goals, but also it was the inception point for the vulnerability disclosure program long-term.

Katie Moussouris: I think one of the trickiest places to get right in scoping is saying, tell us what you think the impact would be of a vulnerability. And this is where disagreements can come about with well-meaning researchers who were reading the rules and saying, okay, well with this credential that I managed to get here, or this token I managed to steal, I don't know what the impact would be unless I try to use it and then potentially pivot through their environment with it, which is usually not allowed, right? But a very technical researcher who is sort of thinking of themselves almost as a red teamer might take it too far. And I remember there were a few cases that required a lot of internal deescalation and some gentle explaining to the researcher by me and others who can speak hacker, of being like, Hey friend, listen, you're totally right. Yep. You can definitely use that to pivot on through, but please do not, and stop it now and no really stop because it's not like you're going to get more money out of it, really we're just saying stop." And luckily nothing bad happened and no researchers got sued or arrested or anything for hacking the Pentagon too much.

Lisa Wiswell Coe: I spoke enough of the language. I had been around the hacker community for probably 10 years prior, having spent a lot of years at DARPA where we had hackers working on particular programs that were like that, but for other objectives. And so, we were out at all of the hacker conferences at the beginning part of the year to try to help them understand that we were really serious about that. It wasn't just some sort of nebulous thing that people that didn't understand them had come up with. And at some point, we decided that it was probably a better place for me if I was detailed to Defense Digital Service because they had the unique authorities to be able to figure out how the hell do we pay for a bug bounty. Who can come up with a quick contract vehicle for them? And some of how we did that, I just drafted a memo for SecDef to sign that said, "We're going to do this and you're supposed to lead, and you got an organization act. Work with her to be able to achieve that, and achieve it successfully." It is really necessary if you're going to show up at the Defense Media Activity and say, "Hey, we're going to hack your shit. For real, we are. Here's the memo that says so."

Alex Romero: This led to conversations around, "Well, we really, really, really need to have a Vulnerability Disclosure Policy for the DoD." That was a huge, gaping hole in our defenses in a sense, because whereas in the physical world, especially after 9/11, we had the See Something, Say Something motto and we invited people to tell us about our faults, the same didn't apply as soon as you were talking about bits and bytes. We, in fact, would invite people to not look at our stuff and have all these very scary banners. "If you don't belong here, go away." Well, that's not how bots on the net think, or that's not how researchers or actual adversaries think. If it's possible, it's going to happen. You just have to think about these things differently.So having a place, a safe place, a safe harbor to protect the researchers so that if they felt that they found something worthwhile to send our way that was bad, they could tell us safely. So to date, we've received over, I want to say, close to 25,000 reports from researchers on vulnerabilities within the DoD of all sorts. It's been a hugely successful program. So I'm a huge proponent of every organization having a security.text file, a security@ email address. Whatever method is best for the researchers, think about it from their perspective. They're just trying to tell you and do the right thing. Don't make their life hard.

> ***"If the first people you're talking to aren't the lawyers, then you've got a problem."***

Alex Rice, left, former Secretary of the Army Eric Fanning, center, and Katie Moussouris.

Lisa Wiswell Coe: I had this mentality that you got to drive it like you stole it. If you're really going to affect change and essentially throw the bowling ball through the window of how we do things, you've got to put your money where your mouth is, otherwise you're just part of the bureaucracy and part of the problem. So if you know how the bureaucracy works, you can find ways to cut corners or to hack it. Break down assumptions and get out of that loop.

Alex Rice: The risks were all around perception and unintended consequences to the hackers. Like, are people going to demonize the hackers? Are they going to be excited to receive the vulnerability reports? Are they going to celebrate it after the fact? Are they going to try to cover it up and not be open about the hackers, found anything? That was one set of it. Is the culture going to be receptive to feedback from hackers. There was a lot of risks around that. And a big chunk of what we focused on was, how do we manage the perception that hackers are good folks, they're here to help.

Katie Moussouris: I think it was definitely a group effort, the folks inside the Pentagon, like Lisa and Charley, absolutely were instrumental, and RoRo, of course, in calming the nerves of the nervous people inside the Pentagon and calming down the hackers was also a group effort. RoRo has a hacking background himself, even before his military service. So he's definitely a native of our pirate-y shores.

Lisa Wiswell Coe: This first thing has got to go perfectly. Otherwise, nothing else will ever be able to go.

Katie Moussouris: So, I think the effect inside the Pentagon was, wow those of us who were against this, we were wrong. But I think the Pentagon really understood the significance of what it had done and understood that in order to maybe inspire the next generation of cyber warriors as they call them, that they needed to show that the Pentagon was a place where you could safely hack and there was a vehicle for it, and that they welcomed it. And I know that the ripple effect throughout other governments was really, really intense as well. Definitely, there were other governments that were interested in launching bug bounties.

Lisa Wiswell Coe: The beautiful part about it is though, they came to a yes quite soon afterwards, after the success of Hack The Pentagon. And for me, I always love it when somebody wants to take credit for something because it means that it went well.

Dino Dai Zovi: I still have a little bit of a chip on my shoulder from all the people that reacted really negatively to (No More Free Bugs), because I think this is a fairly reasonable position. Because of that chip on my shoulder, I do feel kind of justified pointing to things like that and say, "Look, see?"

*Top two inline images courtesy of Katie Moussouris; third image courtesy of Alex Rice.*

Bug Bounty

Defense Digital Service team members and Marines during a live hacking event.