# Why I walked away from $30,000 of DJI bounty money


*This isn't the profession you're looking for*

Kevin Finisterre

Fall 2017

# DJI Full Infrastructure Compromise via GitHub & Amazon s3

*https://www.dji.com/newsroom/news/dji-to-offer-bug-bounty-rewards-for-reporting-software-issues*

## How this all started

Before I get into this story… I want to briefly mention boiler plate email disclaimers. I'll simply point out the sentence 'Are disclaimers "legally useless" as The Economist reports? Probably not, but their effectiveness may be more limited than some believe.' in the Reid & Hellyer Blog post "Email Disclaimers: Legal Effect in American Courts". You may want to delete this PDF after viewing it as it *may* be questionable as to if you are the intended recipient of parts of this document (specifically the contrived CFAA threat letter that is included)!

> This email and any attachments thereto may contain private, confidential, and privileged material for the sole use of the intended recipient. Any review, copying, or distribution of this email (or any attachments thereto) by others is strictly prohibited. If you are not the intended recipient, please contact the sender immediately and permanently delete the original and any copies of this email and any attachments thereto.
> 此电子邮件及附件所包含内容具有机密性，且仅限于接收人使用。未经允许，禁止第三人阅读、复制或传播该电子邮件中的任何信息。如果您不属于以上电子邮件的目标接收者，请您立即通知发送人并删除原电子邮件及其相关的附件。

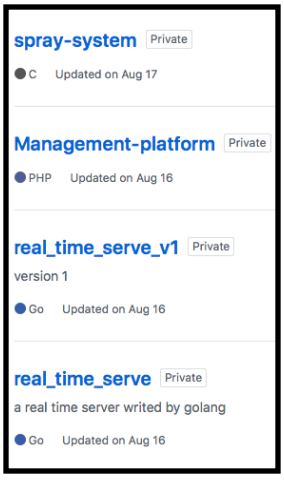
On August 28th 2017 Chinese drone manufacturer Dà-Jiāng Innovations Science and Technology Co., Ltd also known as DJI put forth a press release regarding a new 'Bug Bounty' program known as DJI Threat Identification Reward Program.

> The DJI Threat Identification Reward Program aims to gather insights from researchers and others who discover issues that may create threats to the integrity of our users' private data, such as their personal information or details of the photos, videos and flight logs they create. The program is also seeking vulnerabilities that may reveal proprietary source codes and keys or backdoors created to bypass safety certifications.
>
> Rewards for qualifying bugs will range from $100 to $30,000, depending on the potential impact of the threat. DJI is developing a website with full program terms and a standardized form for reporting potential threats related to DJI's servers, apps or hardware. Starting today, bug reports can be sent to bugbounty@dji.com for review by technical experts.

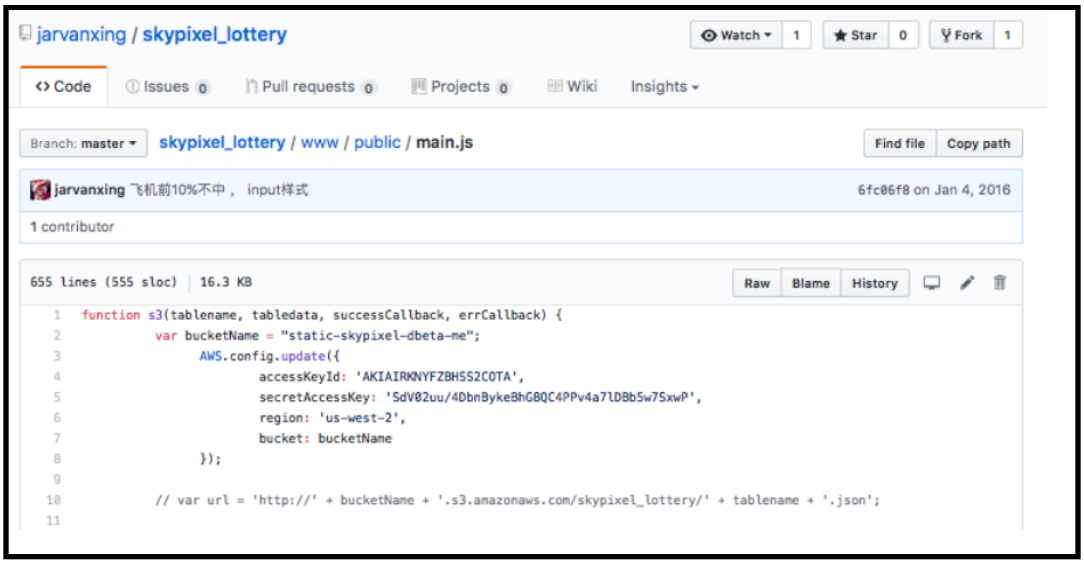
For many of my direct peers the PR surrounding the DJI 'Bug Bounty' program seemed like an attempt to pacify public concerns regarding data privacy issues, coupled with an attempt to quiet down the growing underground DJI drone jailbreaking scene. Several individuals that I know subsequently made attempts at validating the bounty program by submitting bugs of varying pedigrees. I am aware of submissions spanning from hardware based vulnerabilities that impact firmware security, to software based vulnerabilities that impact DJI server integrity, and end user Personally Identifiable Information (PII).

The wording in the DJI press release certainly left a lot to be desired with regard to defined boundaries. One of the first questions I personally had was in regard to the word "servers" in the initial announcement. On Sep 2, 2017 I sent an email to the bugbounty@dji.com email address, with the subject "Clarification of intent on "servers" and their scope in bounty". It took approximately 2 weeks for DJI to respond. Having literally spent the weekend at Derbycon giving a talk about the state of the DJI jailbreaking scene, I came home and realized I had not received a response to the request about servers. Given that many other bounty hunters had literally a month on me time wise, I figured I would begin a little hunt of my own based on what DJI had said publicly when they shared the bounty program.

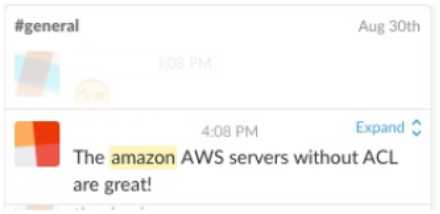
The month prior DJI's SSL keys were disclosed via the GitHub search engine tool. In the past you could use the "in:file" option to hunt for DJI source code, and keys that had been carelessly shared. The image below represents some of the previously public DJI repositories that have been exposed in some cases up to 4 years! DJI SSL keys, and firmware AES keys are among the things that were found.

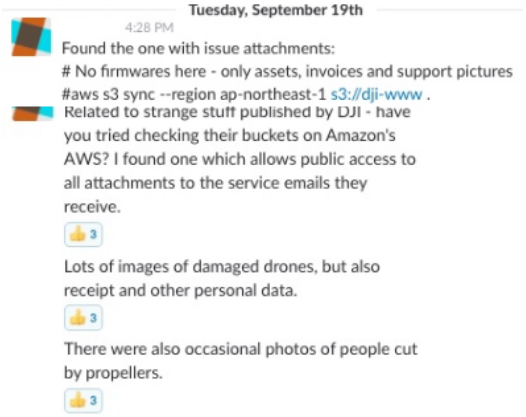


My night of hunting wound up being pretty crazy. Around 4PM Sept 26th JUST before dinner, and family time I wound up finding DJI Skypixel keys for Amazon Web Services (AWS) sitting out in public view! These keys have long since been revoked, but they are depicted below. The repo was named skypixel_lottery… lottery indeed I thought!

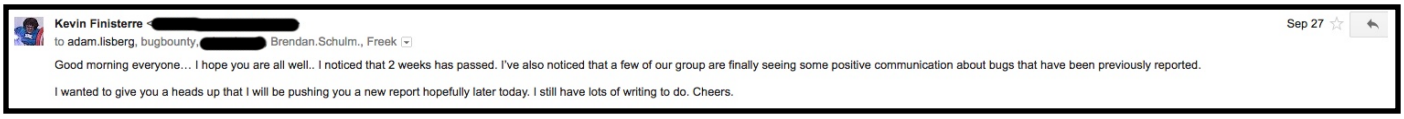



Oddly enough, approximately a week earlier word had spread *further* that some of DJI's AWS buckets were marked with public access, and zero permissions. People had been in and out of slack mentioning it for about a month (literally 2 days after the bounty was announced). Screen shots below show "dji-rev" randoms discussing this fact over the span of 20 days. It is unclear what exactly was in the public DJI buckets, short of the reported: "all attachments to the service emails they receive… images of damaged drones… receipt and other personal data…" and "occasional photos of people cut by propellers.



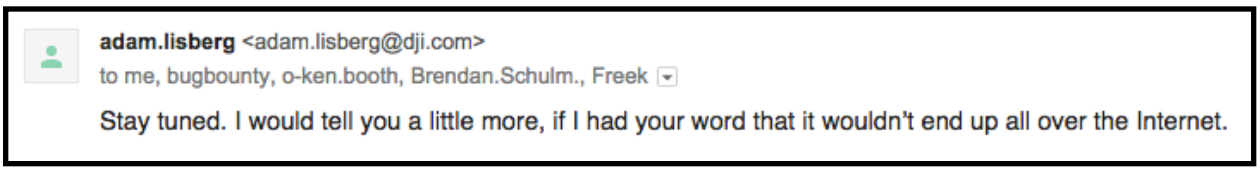
I woke up and sent a semi snarky email about the fact I had not yet seen any response to the "servers" clarification request, and simultaneously gave a preemptive heads up on my incoming bounty submission.. "I noticed that 2 weeks has passed… I wanted to give you a heads up that I will be pushing you a new report hopefully later today. I still have lots of writing to do. Cheers."


Kevin Finisterre <[redacted]>
to adam.lisberg, bugbounty, [redacted] Brendan.Schulm., Freek
Sep 27

Good morning everyone… I hope you are all well.. I noticed that 2 weeks has passed. I've also noticed that a few of our group are finally seeing some positive communication about bugs that have been previously reported.

I wanted to give you a heads up that I will be pushing you a new report hopefully later today. I still have lots of writing to do. Cheers.

Rather than doing something useful… Adam Lisberg chimed and said something semi snarky himself, sort of setting off the tone for future interactions. Never mind the fact we are over a month into dealing with an SSL key leak, and DJI is late on responding about the scope of the bounty, I guess it is time to start getting passive aggressive? I've literally been holding back the fact that their SSL keys had been leaked, and for some reason *now* it seemed like a good idea to imply that I was not trustworthy.


**adam.lisberg** <adam.lisberg@dji.com>
to me, bugbounty, o-ken.booth, Brendan.Schulm., Freek

Stay tuned. I would tell you a little more, if I had your word that it wouldn't end up all over the Internet.

A few hours after Adam and I exchanging words, I finally got a response email to my "servers" question. Please note that DJI had not yet, and still has not made any public definition of the bounty program boundaries, and terms. It should also be noted that to this day DJI has yet to publish a rule guide, or roadmap for bounty. The response to my question about DJI "servers" being in scope read as follows:

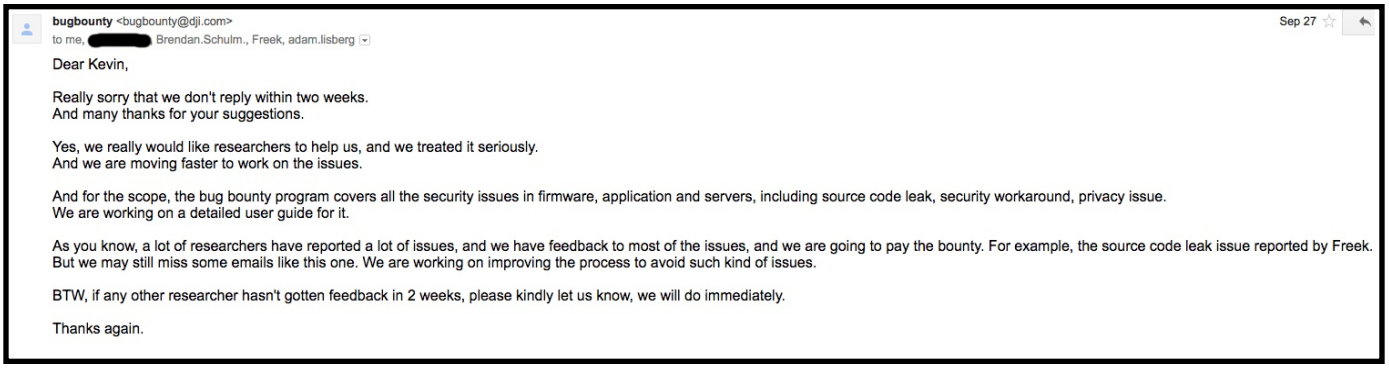
*"Really sorry that we don't reply within two weeks. And many thanks for your suggestions. Yes, we really would like researchers to help us…* ***for the scope, the bug bounty program covers all the security issues in firmware, application and servers, including source code leak, security workaround, privacy issue****. We are*

*working on a detailed user guide for it.*

*As you know, a lot of researchers have reported a lot of issues, and we have feedback to most of the issues, and we are going to pay the bounty. For example, the source code leak issue reported by Freek.*
*But we may still miss some emails like this one. We are working on improving the process to avoid such kind of issues.*

*BTW, if any other researcher hasn't gotten feedback in 2 weeks, please kindly let us know, we will do immediately. Thanks again."*

Pay particular attention to the portion of the email response that I bolded, and underlined. For your viewing pleasure, I have also included an image of the email below. DJI made it very clear that their servers were in scope, likewise they made it very clear that "source code leaks" were in scope. I won't go into details in this paper, but a group of the "dji-rev" Slack "Original Gangsters" aka "OGs" were already in communications with DJI about the fact their SSL key had been leaked on GitHub earlier in the month, having been exposed for several years.



**bugbounty** <bugbounty@dji.com> Sep 27

to me, [redacted] Brendan.Schulm., Freek, adam.lisberg

Dear Kevin,

Really sorry that we don't reply within two weeks.
And many thanks for your suggestions.

Yes, we really would like researchers to help us, and we treated it seriously.
And we are moving faster to work on the issues.

And for the scope, the bug bounty program covers all the security issues in firmware, application and servers, including source code leak, security workaround, privacy issue.
We are working on a detailed user guide for it.

As you know, a lot of researchers have reported a lot of issues, and we have feedback to most of the issues, and we are going to pay the bounty. For example, the source code leak issue reported by Freek.
But we may still miss some emails like this one. We are working on improving the process to avoid such kind of issues.

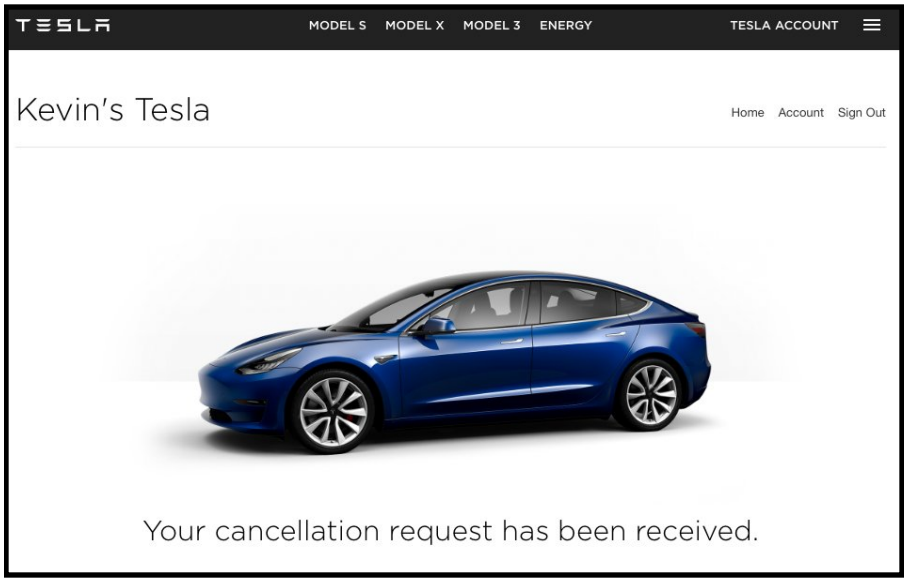
BTW, if any other researcher hasn't gotten feedback in 2 weeks, please kindly let us know, we will do immediately.

Thanks again.

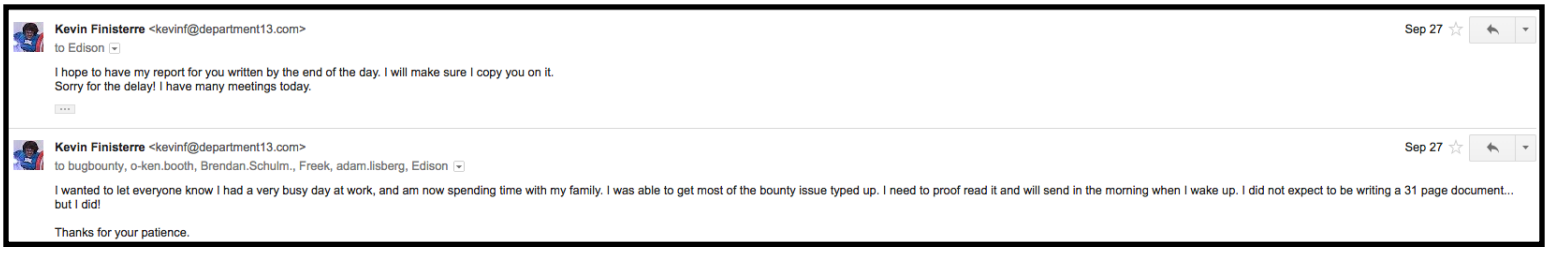
By 1:21:52 PM Sept 27th DJI had sent the reply pictured above. I spent the next few hours examining the impact of what had been exposed on their AWS servers and began typing up my bounty report. I had no clue what a rabbit hole it would turn out to be!

Lets take a little side bar, do you wanna get you some bounty loot? Ask yourself what it is worth to you to devalue your time for a fraction of the pay you'd normally receive. Ask yourself what YOU are worth… do you know your own hourly bill rate? Do you know what you would charge for a week of work plus a report? How about post work *complimentary* support? If you have no clue what I am talking about, you should think about your time as a potential bounty hunter more wisely. $30,000 is a lot of loot… what would you do with it?

I was gonna buy me a sick Tesla Model 3. Please note, I've since had to cancel the order. Don't forget this isn't a happy bounty story. Please pour out some liquor for the Model 3 that will never be.




The amount of things that needed written up wound up being enormous. In the end I would up with a 31 page report when it was all said and done. I wound up asking for some extra to write the bug up to highlights the ramifications properly.



In the mean time I passed some basic information on via a friend at DJI with a better technical understanding than the people I was dealing with. A few hours later I got a response back from Edison Yongsen Chen. I had let them know about the fact I had seen unencrypted flight logs, passports, drivers licenses, and Identification Cards. As you can see below the response from Edison acknowledges the existence of said data, and asks for help. This was the first in a long line of education on basic security concepts, and bug bounty practices. Over 130 emails were exchanged back and forth at one point in one thread. At one point days later DJI even offered to hire me directly to consult with them on their security.

**Kevin Finisterre** <kevinf@department13.com>
to bugbounty, o-ken.booth, Brendan.Schulm., Freek, adam.lisberg

Thank you for your time. I hope to have the current issue written up properly by the end of the day.
Cheers.

**Edison Chen** <yongsen.chen@dji.com>
to me

Dear Kevin,

We checked the code of server, and found it's not easy to get the flight log and VISA pictures.

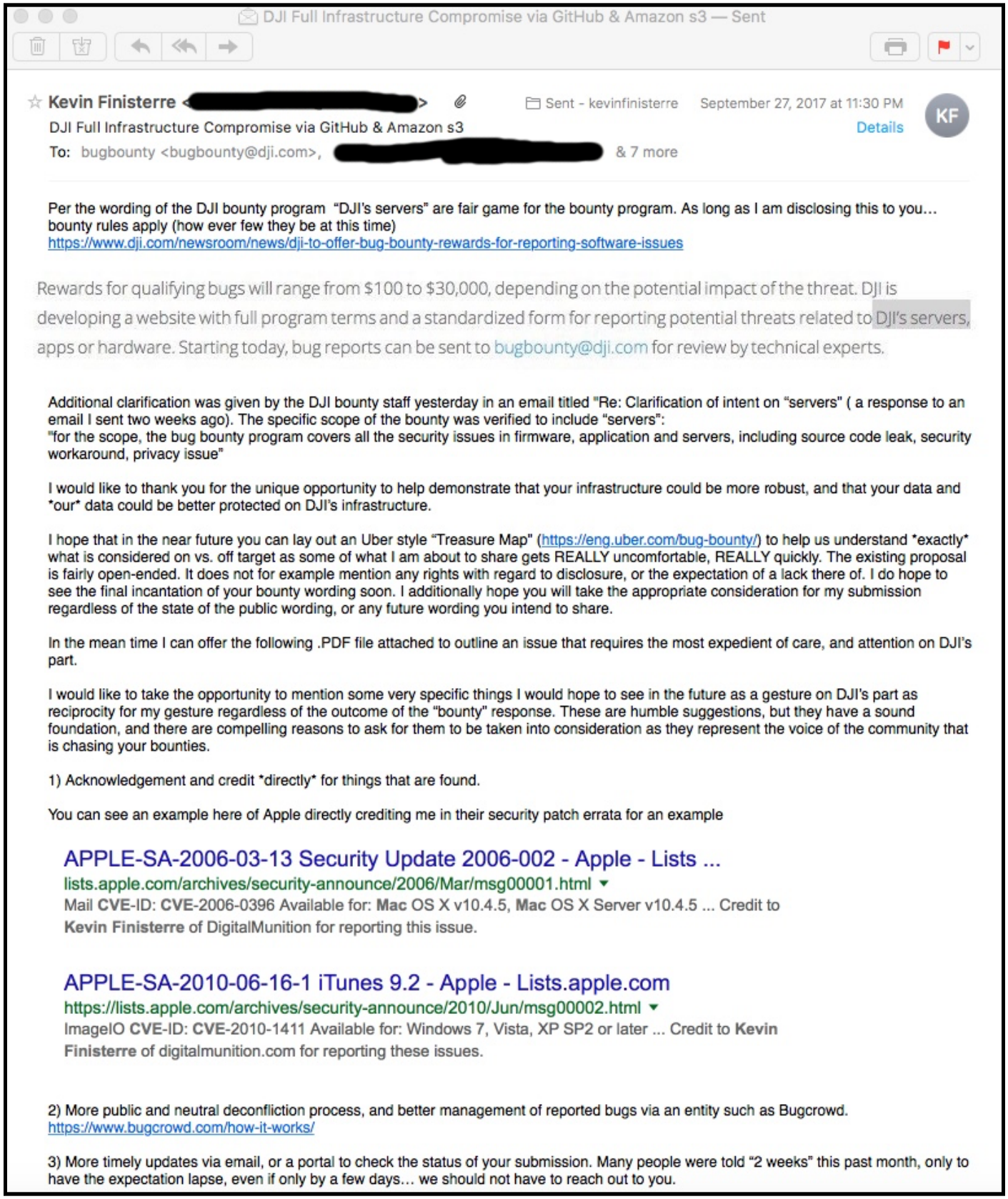
Could you share some hint for how to do that?

Truly appreciate for that!

---
Best Regards,

Yongsen Chen / 陈永森

The following pictures represent the bounty submission email I sent to DJI at 11:30PM on Sept 27th. I literally spent all night making sure it was written up properly, and highlighting very specific areas of concern with regard to DJI's security posture.



DJI Full Infrastructure Compromise via GitHub & Amazon s3 — Sent

☆ **Kevin Finisterre** <[redacted]> Sent - kevinfinisterre September 27, 2017 at 11:30 PM

DJI Full Infrastructure Compromise via GitHub & Amazon s3 Details

To: bugbounty <bugbounty@dji.com>, [redacted] & 7 more

KF

Per the wording of the DJI bounty program "DJI's servers" are fair game for the bounty program. As long as I am disclosing this to you… bounty rules apply (how ever few they be at this time)
https://www.dji.com/newsroom/news/dji-to-offer-bug-bounty-rewards-for-reporting-software-issues

Rewards for qualifying bugs will range from $100 to $30,000, depending on the potential impact of the threat. DJI is developing a website with full program terms and a standardized form for reporting potential threats related to DJI's servers, apps or hardware. Starting today, bug reports can be sent to bugbounty@dji.com for review by technical experts.

Additional clarification was given by the DJI bounty staff yesterday in an email titled "Re: Clarification of intent on "servers" ( a response to an email I sent two weeks ago). The specific scope of the bounty was verified to include "servers":
"for the scope, the bug bounty program covers all the security issues in firmware, application and servers, including source code leak, security workaround, privacy issue"

I would like to thank you for the unique opportunity to help demonstrate that your infrastructure could be more robust, and that your data and *our* data could be better protected on DJI's infrastructure.

I hope that in the near future you can lay out an Uber style "Treasure Map" (https://eng.uber.com/bug-bounty/) to help us understand *exactly* what is considered on vs. off target as some of what I am about to share gets REALLY uncomfortable, REALLY quickly. The existing proposal is fairly open-ended. It does not for example mention any rights with regard to disclosure, or the expectation of a lack there of. I do hope to see the final incantation of your bounty wording soon. I additionally hope you will take the appropriate consideration for my submission regardless of the state of the public wording, or any future wording you intend to share.

In the mean time I can offer the following .PDF file attached to outline an issue that requires the most expedient of care, and attention on DJI's part.

I would like to take the opportunity to mention some very specific things I would hope to see in the future as a gesture on DJI's part as reciprocity for my gesture regardless of the outcome of the "bounty" response. These are humble suggestions, but they have a sound foundation, and there are compelling reasons to ask for them to be taken into consideration as they represent the voice of the community that is chasing your bounties.

1) Acknowledgement and credit *directly* for things that are found.

You can see an example here of Apple directly crediting me in their security patch errata for an example

APPLE-SA-2006-03-13 Security Update 2006-002 - Apple - Lists ...
lists.apple.com/archives/security-announce/2006/Mar/msg00001.html
Mail **CVE**-ID: **CVE**-2006-0396 Available for: **Mac** OS X v10.4.5, **Mac** OS X Server v10.4.5 ... Credit to **Kevin Finisterre** of DigitalMunition for reporting this issue.

APPLE-SA-2010-06-16-1 iTunes 9.2 - Apple - Lists.apple.com
https://lists.apple.com/archives/security-announce/2010/Jun/msg00002.html
ImageIO **CVE**-ID: **CVE**-2010-1411 Available for: Windows 7, Vista, XP SP2 or later ... Credit to **Kevin Finisterre** of digitalmunition.com for reporting these issues.

2) More public and neutral deconfliction process, and better management of reported bugs via an entity such as Bugcrowd.
https://www.bugcrowd.com/how-it-works/

3) More timely updates via email, or a portal to check the status of your submission. Many people were told "2 weeks" this past month, only to have the expectation lapse, even if only by a few days… we should not have to reach out to you.

4) Solid detail on the "right to disclose" as many researchers seek as part of the process of gaining "credit" for the work. Information is usually embargoed until the vendor has a reasonable chance to fix it, at which point the vulnerability can be shared publicly. Understandably improperly embargoed info can impact ones ability to enjoy a bounty.

Example:
https://www.scmagazineuk.com/pen-testers-discover-mega-vulnerabilities-in-uber/article/530467/
Eight new vulnerabilities were reported by the team (four are under embargo, not to be disclosed until later): brute force attack to get invite codes via riders.uber.com, view driver waybill via drivers UUID, get drivers private email from UUID and getting information on trips from arbitrary users.

5) Public disclosure, and proper notification by DJI to the Public about discovered vulnerabilities with transparency.
"DJI Enhances Software Security In Its Flight Control Apps" was semi offensive to some folks as it hardly put emphasis into thanking the group for our hard work, and our choice to disclose.
http://www.dji.com/newsroom/news/dji-enhances-software-security-in-its-flight-control-apps

'Recent work by DJI's software security team and external researchers has discovered that JPush also collects extraneous packets of data, which include a list of apps installed on the user's Android device, and sends them to JPush's server. DJI did not authorize or condone either the collection or transmission of this data, and DJI never accessed this data. JPush has been removed from our apps, and DJI will develop new methods for providing app status updates that better protect our customers' data.'
^— This paragraph does not give the group justice, and "thanks" certainly was not conveyed.

More importantly the recent SSL certificate compromise has not been shared with your end users. First, it is the right thing to do, with regard to disclosing breaches, or "potential breach". Second in some cases where PII (Personally Identifiable Information) is located and "potentially" could have been disclosed to 3rd parties it is of the upmost importance to make sure you fulfill your legal obligations to notify the folks that are / may have been impacted.

Here is an example for the State of Arizona (One of the ID's pulled from your server cache in the below document is from the Arizona… ) I don not know if it is considered that you are "conducting business in Arizona" when you interact with the person or not, but here is an example of Arizona notification law… http://law.justia.com/codes/arizona/2015/title-44/section-44-7501

2015 Arizona Revised Statutes
Title 44 - Trade and Commerce
§ 44-7501 Notification of breach of security system; enforcement; civil penalty; preemption; exceptions; definitions

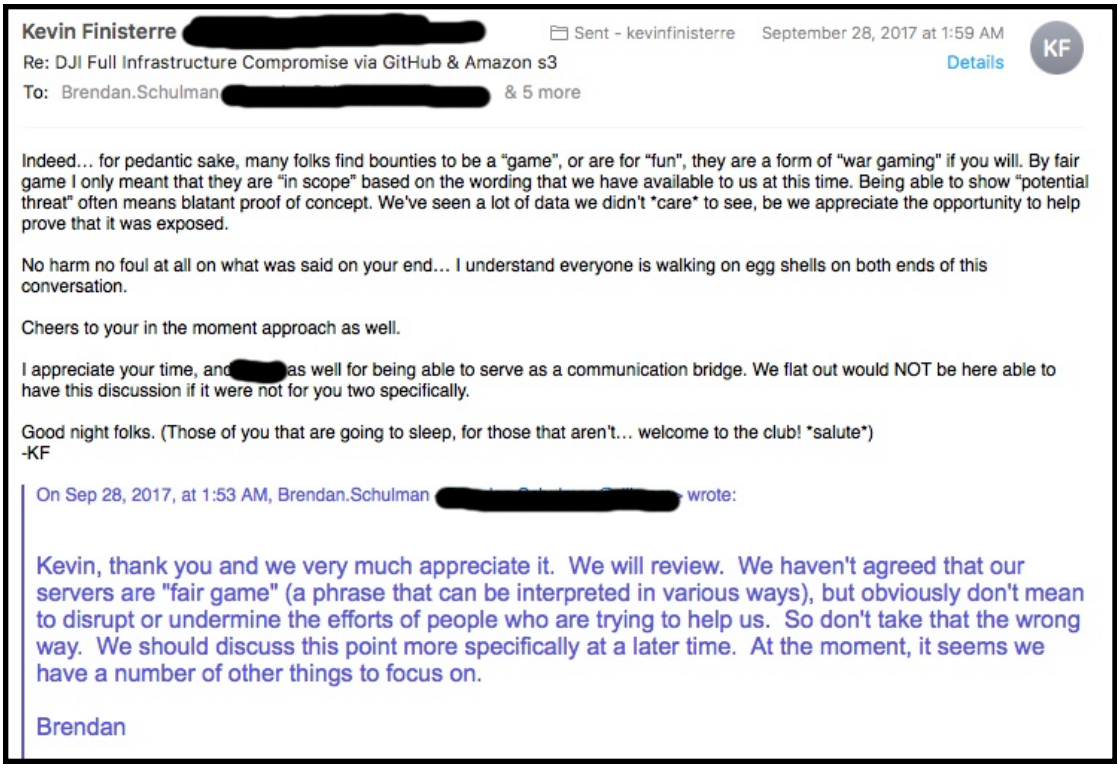
I appreciate your time, and do hope you understand the importance of the data I am presenting you, and I hope you understand the ramifications of not properly notifying the public of your data breaches.

Thanks for your time.

Kevin Finisterre
[redacted]

DJIUnobtanium V2.pdf

The first email I got back was from Brendan Schulman immediately debating the fact that the "servers" were *not* what I called "fair game". I further explained what I meant with a semi pedantic reply depicted below in the following screenshot.



**Kevin Finisterre** [redacted] Sent - kevinfinisterre September 28, 2017 at 1:59 AM

Re: DJI Full Infrastructure Compromise via GitHub & Amazon s3 Details

To: Brendan.Schulman [redacted] & 5 more

Indeed… for pedantic sake, many folks find bounties to be a "game", or are for "fun", they are a form of "war gaming" if you will. By fair game I only meant that they are "in scope" based on the wording that we have available to us at this time. Being able to show "potential threat" often means blatant proof of concept. We've seen a lot of data we didn't *care* to see, be we appreciate the opportunity to help prove that it was exposed.

No harm no foul at all on what was said on your end… I understand everyone is walking on egg shells on both ends of this conversation.

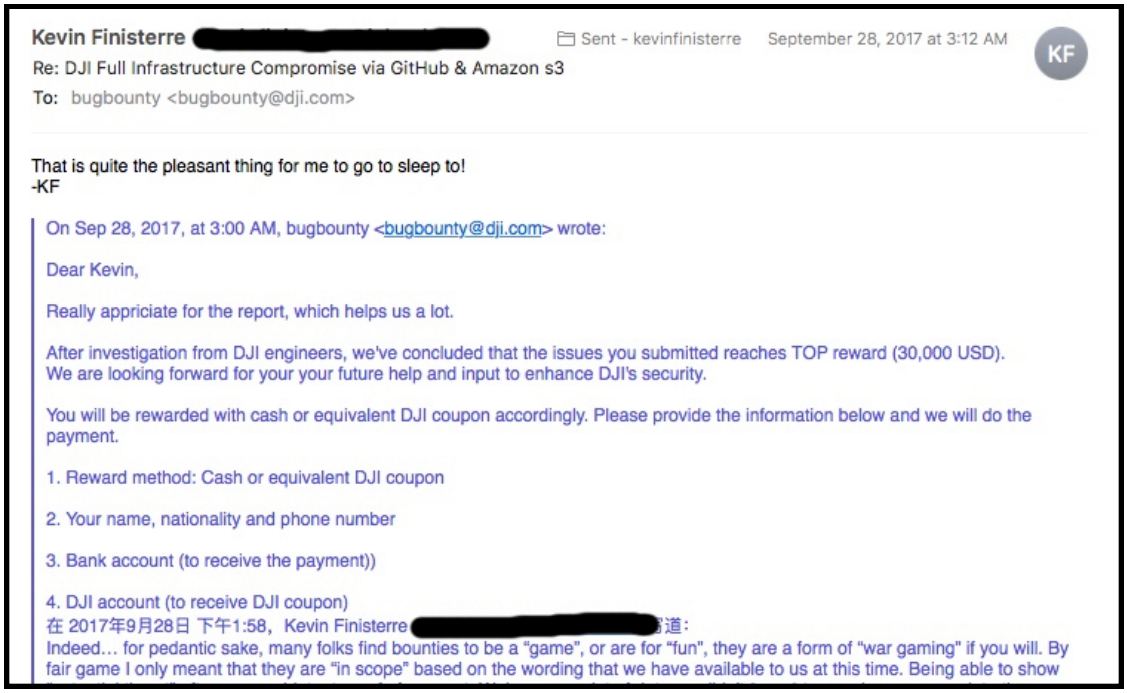
Cheers to your in the moment approach as well.

I appreciate your time, and [redacted]as well for being able to serve as a communication bridge. We flat out would NOT be here able to have this discussion if it were not for you two specifically.

Good night folks. (Those of you that are going to sleep, for those that aren't… welcome to the club! *salute*)
-KF

> On Sep 28, 2017, at 1:53 AM, Brendan.Schulman [redacted] wrote:
>
> Kevin, thank you and we very much appreciate it. We will review. We haven't agreed that our servers are "fair game" (a phrase that can be interpreted in various ways), but obviously don't mean to disrupt or undermine the efforts of people who are trying to help us. So don't take that the wrong way. We should discuss this point more specifically at a later time. At the moment, it seems we have a number of other things to focus on.
>
> Brendan

A little over an hour later I received the following email stating that DJI has "concluded that the issues [I] submitted reached TOP reward (30,000 USD)" and that I "will be rewarded with cash".



**Kevin Finisterre** [redacted] Sent - kevinfinisterre September 28, 2017 at 3:12 AM

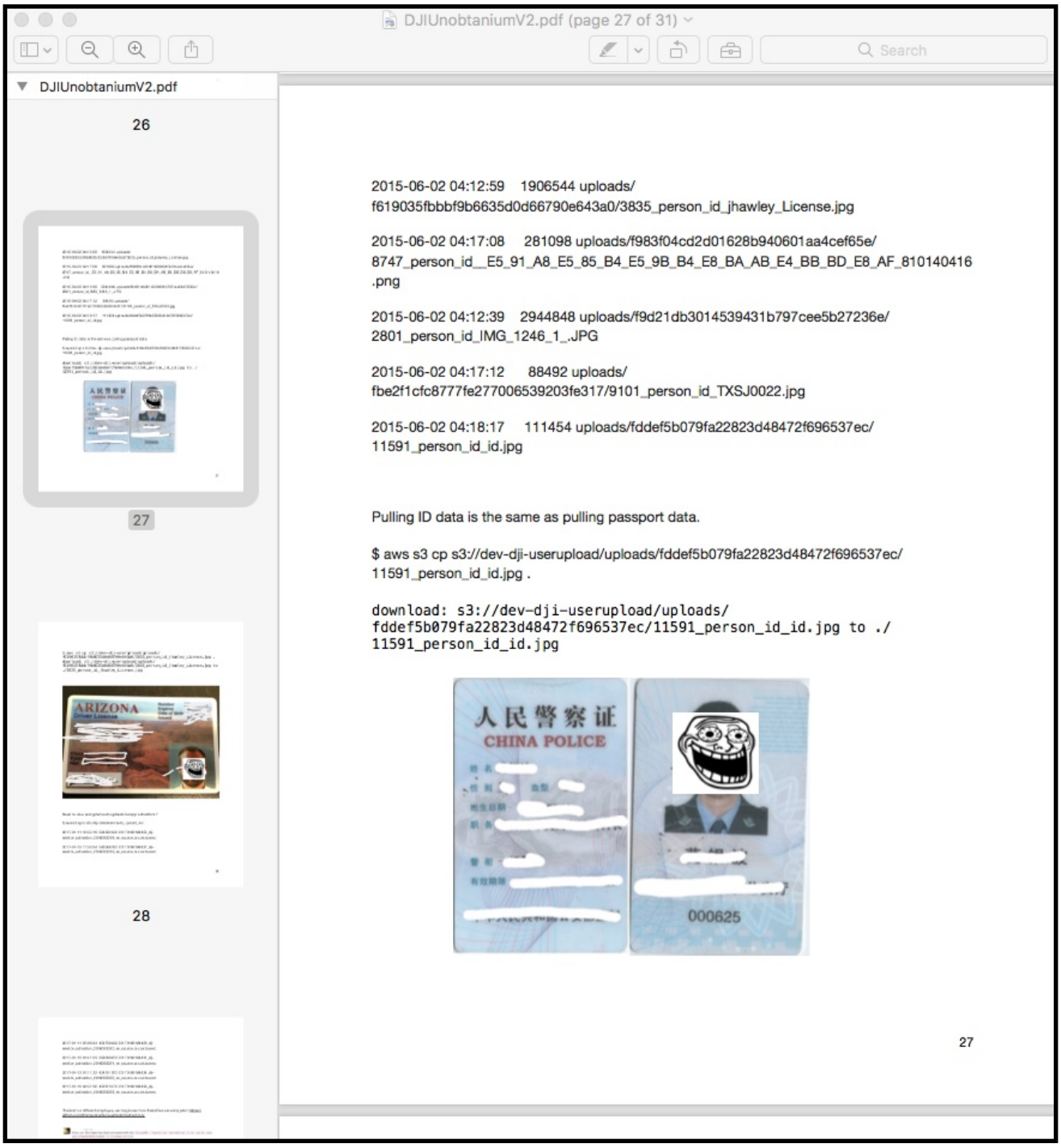
Re: DJI Full Infrastructure Compromise via GitHub & Amazon s3

To: bugbounty <bugbounty@dji.com>

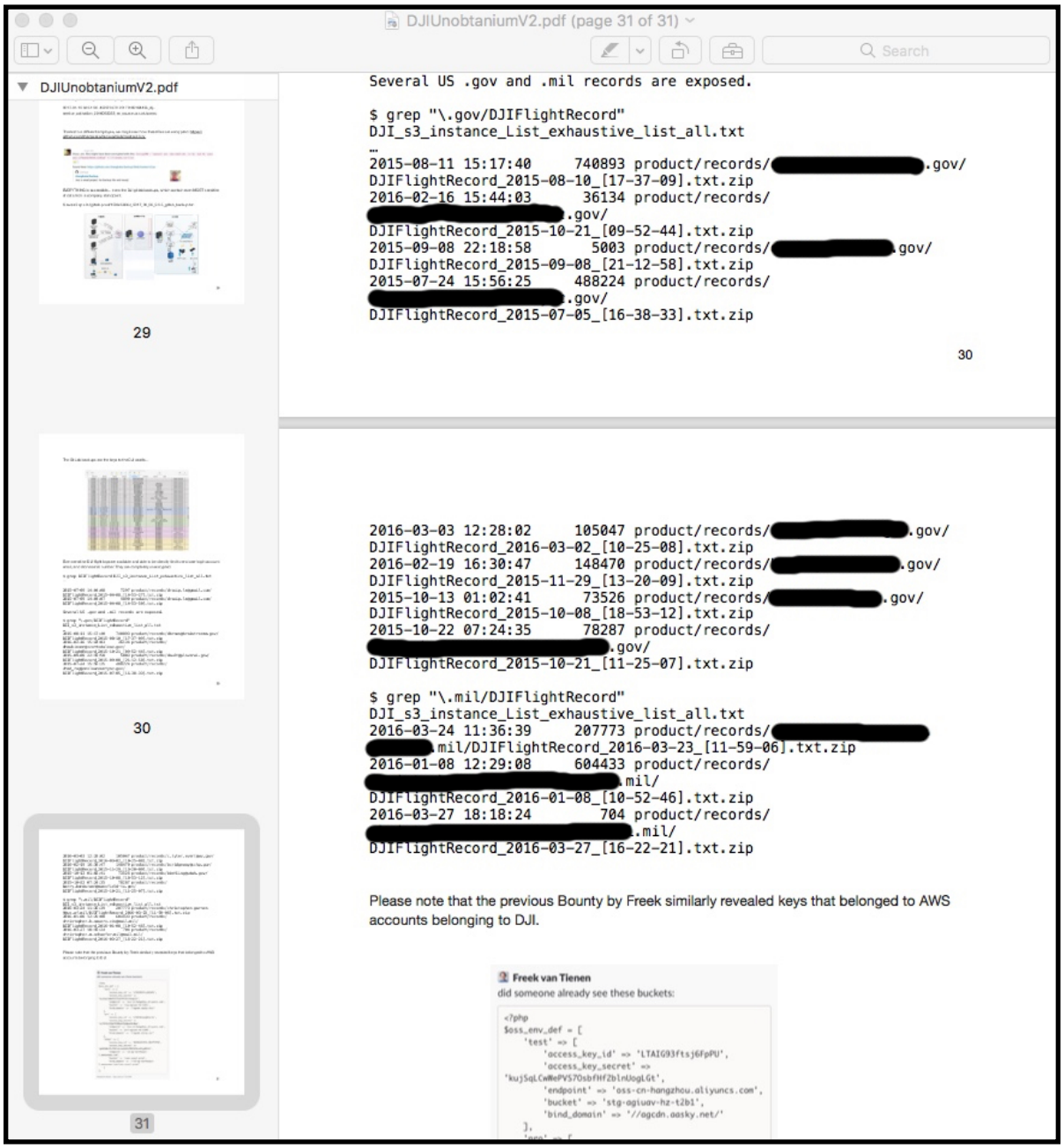
That is quite the pleasant thing for me to go to sleep to!
-KF

> On Sep 28, 2017, at 3:00 AM, bugbounty <bugbounty@dji.com> wrote:
>
> Dear Kevin,
>
> Really appriciate for the report, which helps us a lot.
>
> After investigation from DJI engineers, we've concluded that the issues you submitted reaches TOP reward (30,000 USD).
> We are looking forward for your your future help and input to enhance DJI's security.
>
> You will be rewarded with cash or equivalent DJI coupon accordingly. Please provide the information below and we will do the payment.
>
> 1. Reward method: Cash or equivalent DJI coupon
>
> 2. Your name, nationality and phone number
>
> 3. Bank account (to receive the payment))
>
> 4. DJI account (to receive DJI coupon)
> 在 2017年9月28日 下午1:58，Kevin Finisterre [redacted]道:
> Indeed… for pedantic sake, many folks find bounties to be a "game", or are for "fun", they are a form of "war gaming" if you will. By fair game I only meant that they are "in scope" based on the wording that we have available to us at this time. Being able to show

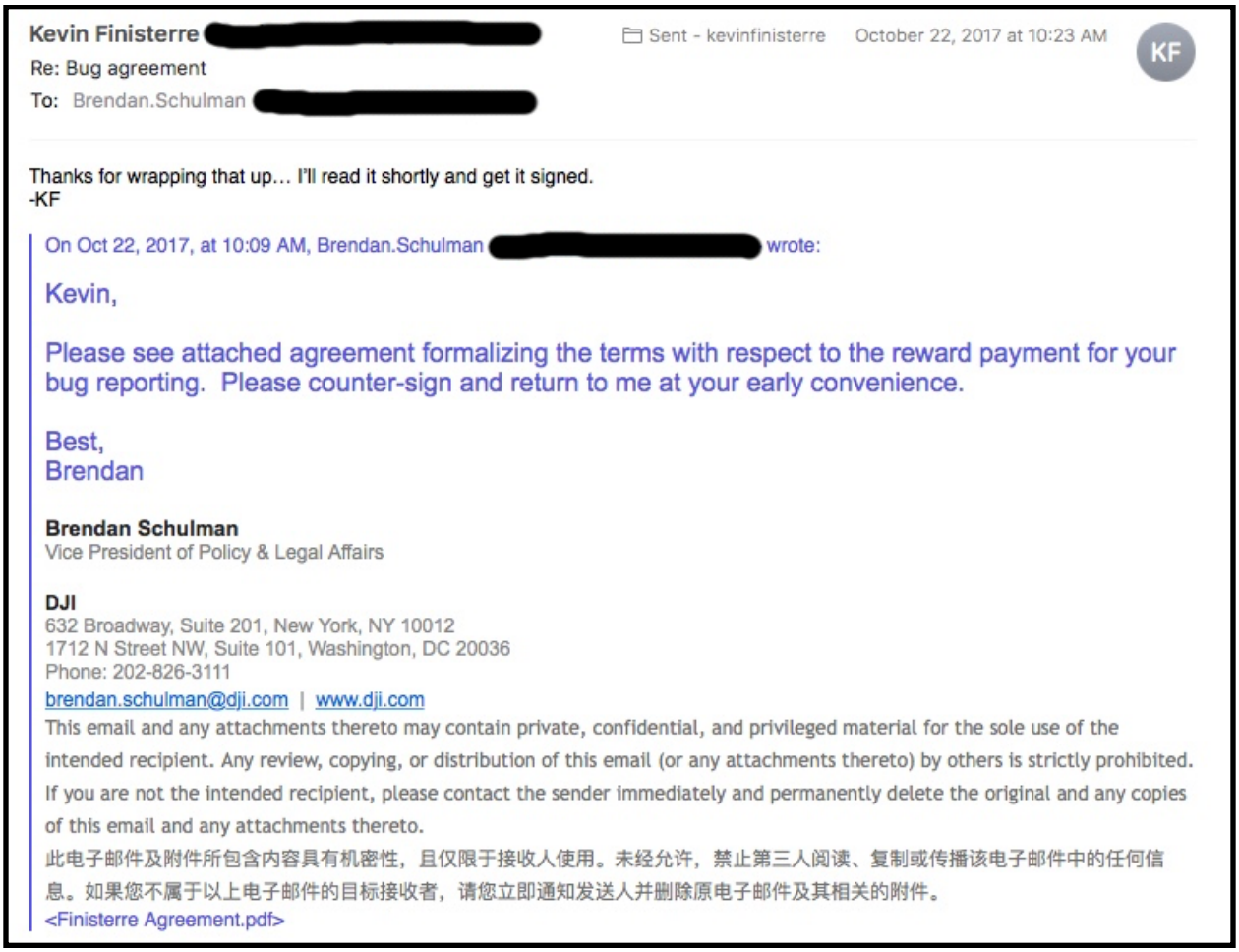
The report I had delivered was in standard PDF form and covered all aspects of what I found, including but not limited to passport data, drivers licenses, state identification, and flight logs. Once I get a proper redaction tool I will release it.



There were serious ramifications to the things that were found on the DJI AWS servers. One of the first things I did to judge the impact of the exposure was grep for ".mil" and ".gov", "gov.au". Immediately flight logs for a number of potentially sensitive locations came out. It should be noted that newer logs, and PII seemed to be encrypted with a static OpenSSL password, so theoretically some of the data was at least loosely protected from prying eyes. Unfortunately the rest of the server side security renders this point moot.



What follows can only be described as a comedy of errors… Nearly a month later on October 22nd the terms for my particular bounty "Bug agreement" finally showed up. Several of my peers also received similar terms letters. The letter was literally not sign-able, and I began working on ways to soften the tone and make it more appropriate. This is the point at which you may want to delete this PDF, or consult your lawyer on the how enforceable boiler plate email disclaimers are.



**Kevin Finisterre** [redacted] Sent - kevinfinisterre October 22, 2017 at 10:23 AM

Re: Bug agreement

To: Brendan.Schulman [redacted]

Thanks for wrapping that up… I'll read it shortly and get it signed.
-KF

On Oct 22, 2017, at 10:09 AM, Brendan.Schulman [redacted] wrote:

Kevin,

Please see attached agreement formalizing the terms with respect to the reward payment for your bug reporting. Please counter-sign and return to me at your early convenience.

Best,
Brendan

**Brendan Schulman**
Vice President of Policy & Legal Affairs

**DJI**
632 Broadway, Suite 201, New York, NY 10012
1712 N Street NW, Suite 101, Washington, DC 20036
Phone: 202-826-3111
brendan.schulman@dji.com | www.dji.com

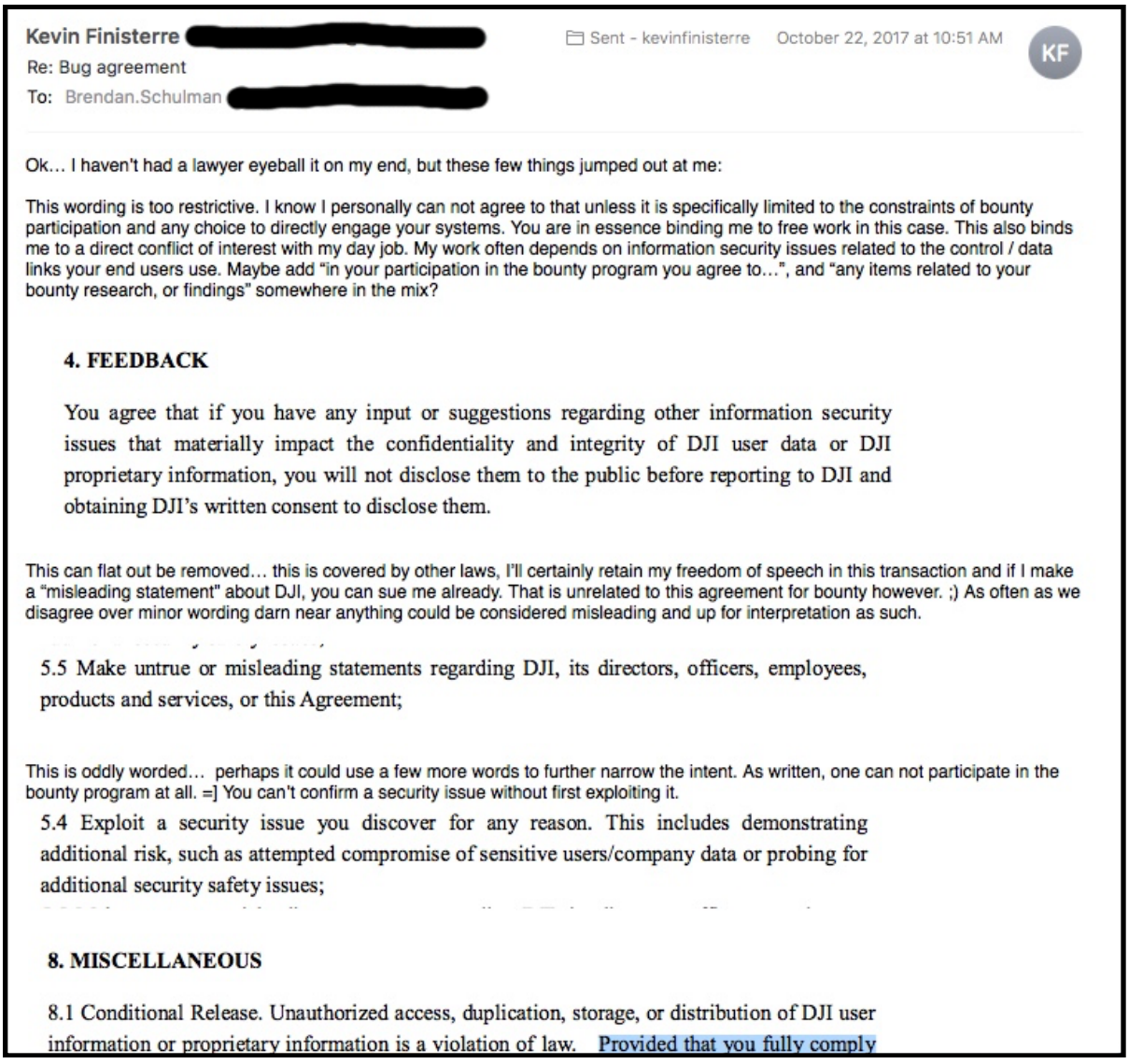
This email and any attachments thereto may contain private, confidential, and privileged material for the sole use of the intended recipient. Any review, copying, or distribution of this email (or any attachments thereto) by others is strictly prohibited. If you are not the intended recipient, please contact the sender immediately and permanently delete the original and any copies of this email and any attachments thereto.

此电子邮件及附件所包含内容具有机密性，且仅限于接收人使用。未经允许，禁止第三人阅读、复制或传播该电子邮件中的任何信息。如果您不属于以上电子邮件的目标接收者，请您立即通知发送人并删除原电子邮件及其相关的附件。

<Finisterre Agreement.pdf>

I won't go into too much detail, but the agreement that was put in front of me by DJI in essence did not offer researchers any sort of protection. For me personally the wording put my right to work at risk, and posed a direct conflicts of interest to many things including my freedom of speech. It almost seemed like a joke. It was pretty clear the entire 'Bug Bounty' program was rushed based on this alone.

Several progressions were made in making the wording more acceptable, I must actually credit Brendan Schulman on attempting to serve as a communication bridge between myself and his Chinese counterparts in the legal department in Guangdong. Unfortunately he was not able to keep the barbarians at the gate, and I received a thinly veiled Computer Fraud and Abuse Act threat from DJI.



Kevin Finisterre [redacted] Sent - kevinfinisterre October 22, 2017 at 10:51 AM KF

Re: Bug agreement

To: Brendan.Schulman [redacted]

Ok... I haven't had a lawyer eyeball it on my end, but these few things jumped out at me:

This wording is too restrictive. I know I personally can not agree to that unless it is specifically limited to the constraints of bounty participation and any choice to directly engage your systems. You are in essence binding me to free work in this case. This also binds me to a direct conflict of interest with my day job. My work often depends on information security issues related to the control / data links your end users use. Maybe add "in your participation in the bounty program you agree to...", and "any items related to your bounty research, or findings" somewhere in the mix?

**4. FEEDBACK**

You agree that if you have any input or suggestions regarding other information security issues that materially impact the confidentiality and integrity of DJI user data or DJI proprietary information, you will not disclose them to the public before reporting to DJI and obtaining DJI's written consent to disclose them.

This can flat out be removed... this is covered by other laws, I'll certainly retain my freedom of speech in this transaction and if I make a "misleading statement" about DJI, you can sue me already. That is unrelated to this agreement for bounty however. ;) As often as we disagree over minor wording darn near anything could be considered misleading and up for interpretation as such.

5.5 Make untrue or misleading statements regarding DJI, its directors, officers, employees, products and services, or this Agreement;

This is oddly worded... perhaps it could use a few more words to further narrow the intent. As written, one can not participate in the bounty program at all. =] You can't confirm a security issue without first exploiting it.

5.4 Exploit a security issue you discover for any reason. This includes demonstrating additional risk, such as attempted compromise of sensitive users/company data or probing for additional security safety issues;

**8. MISCELLANEOUS**

8.1 Conditional Release. Unauthorized access, duplication, storage, or distribution of DJI user information or proprietary information is a violation of law. Provided that you fully comply

Somehow, despite discussing it briefly with Brendan I completely missed reading the letter sent on October 27th, and I negotiated other changes to the agreement wording in good faith via phone. Perhaps it was the suggestion to "focus on what is important" (the money! lol)? I honestly have no clue how I missed the CFAA threat in full!

Demand Letter_Finisterre_102717.pdf (1 page)

Search

THE FUTURE OF POSSIBLE

October 27, 2017

Legal Department
SZ DJI Technology Co., Ltd.
18 Gaoxin S. 4th Ave.
Shenzhen, Guangdong
China

Mr. Kevin Finisterre
[redacted]

Re: DJI Bug Bounty Program

Dear Mr. Finisterre,

Thank you for your report to DJI regarding an information security issue. While we appreciate your support, DJI's legal department noticed that you had obtained DJI proprietary and confidential information by accessing DJI server without authorization on or about September 27, 2017, which caused damage to the integrity of the server and aforementioned information. Without waiving other rights under applicable laws, DJI hereby demands you to immediately delete and destroy any copies of information you obtained from such unauthorized access in a complete and irrevocable way.

Please note that your report to DJI and correspondence therefor do not constitute DJI's grant of authorization to you. This could be evidenced by the DJI Bug Bounty Program agreement that DJI has been discussing with you since receiving your report. In addition, in the email dated September 2, 2017 that is followed by your report email dated September 27, 2017, you acknowledged that people who wanted to participate in the DJI Bug Bounty Program do not have authority to access DJI servers: "[y]ou will note that elaborate bugs like this [cannot] be exposed if researchers are prevented from accessing the infrastructure…in theory more bounty worthy bugs could be disclosed IF researchers are allowed to continue."

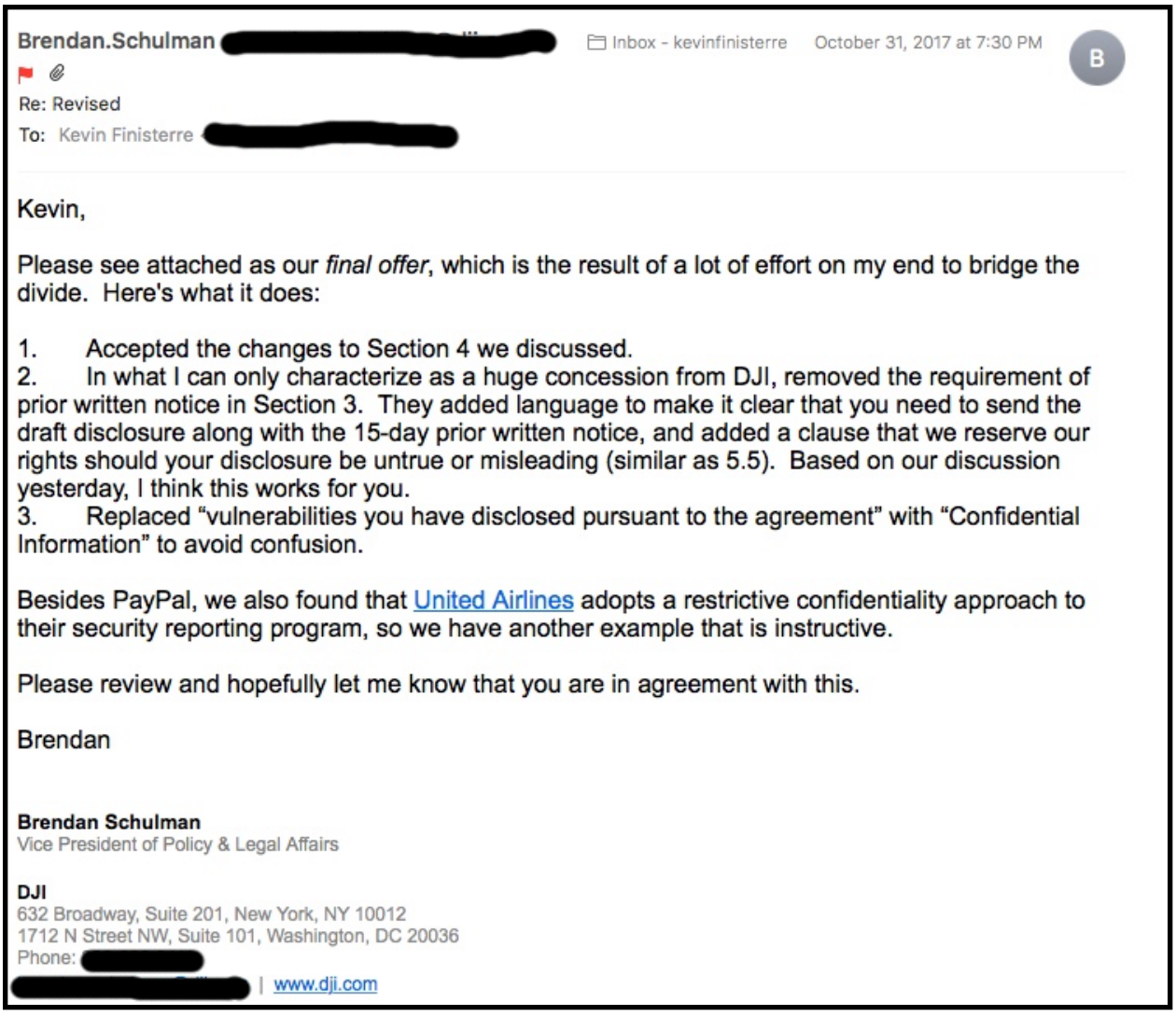
Please be advised that DJI is in good faith willing to explore the possibility of reaching an amicable resolution regarding the aforementioned unauthorized access and transmission of information, including a release of liability agreed by both parties. In the interim, DJI reserves all rights under applicable laws, including but not limited to, its right of action under the Computer Fraud and Abuse Act.

Should you have any questions, please contact us at legal@dji.com.

Sincerely,

DJI Legal Department

Having completely missed the previous snarky and offensive commentary, Brendan and I negotiated the following "final offer" in terms. I of course still needed to have a lawyer review the terms, even if they were DJI's final offer. In the days following no less than 4 lawyers told me in various ways that the agreement was not only extremely risky, but was likely crafted in bad faith to silence anyone that signed it. I went through various iterations to get the letter corrected. It was ultimately going to cost me several thousand dollars for a lawyer that I was confident could cover all angles to put my concerns to bed and make the agreement sign-able.



**Brendan.Schulman** [redacted] Inbox - kevinfinisterre October 31, 2017 at 7:30 PM

Re: Revised

To: Kevin Finisterre [redacted]

Kevin,

Please see attached as our *final offer*, which is the result of a lot of effort on my end to bridge the divide. Here's what it does:

1. Accepted the changes to Section 4 we discussed.
2. In what I can only characterize as a huge concession from DJI, removed the requirement of prior written notice in Section 3. They added language to make it clear that you need to send the draft disclosure along with the 15-day prior written notice, and added a clause that we reserve our rights should your disclosure be untrue or misleading (similar as 5.5). Based on our discussion yesterday, I think this works for you.
3. Replaced "vulnerabilities you have disclosed pursuant to the agreement" with "Confidential Information" to avoid confusion.

Besides PayPal, we also found that United Airlines adopts a restrictive confidentiality approach to their security reporting program, so we have another example that is instructive.

Please review and hopefully let me know that you are in agreement with this.

Brendan

**Brendan Schulman**
Vice President of Policy & Legal Affairs

**DJI**
632 Broadway, Suite 201, New York, NY 10012
1712 N Street NW, Suite 101, Washington, DC 20036
Phone: [redacted]
[redacted] | www.dji.com

At this point I think I realized how much time I had wasted, and how offensive this "dick move" was. I sent out a few more snarky emails to all of the folks involved in the bounty handling and let everyone know exactly how offended I was. I eventually asked for an apology, and suggested that unless something changed then I would simply need to walk away from the program and the bounty completely. Today is pretty much the following day of me having said that… it is nearly 5am, and I stayed up all night typing this.

I honestly don't have any more time to waste… I may not even spell check, or grammar this document, as it isn't worth my effort. I'm pretty sure I even forgot to redact an email address or two. I can't be bothered. It is bed time! There is of course much more to this story, but I don't have the patience to tell it at the moment. Let this serve as a warning to all ye who seek bounty loot, especially from DJI.

If you that are wondering if DJI even bothered to respond after I got offended over the CFAA threat, you should be happy to know it was flat out radio silence from there on out. All Twitter DM's stopped, SMS messages went unanswered, etc. Cold blooded silence.

Thanks for listening. If something sounds too good to be true, it probably is.