Q So Ms. Tavenner at the hearing was clear. She said that, we will have the highest degree of security and privacy protection. So are you testifying today that there was no way to make the system more secure and better protect people's privacy?

A I can't speak to what Marilyn is referring to as the highest. I think in the world of FISMA and abiding by the security controls that are prescribed under FISMA, highest means that it passes those security controls without any high findings. That's the practical interpretation of highest level of security. It meets FISMA requirements.

Q Which level of FISMA? FISMA moderate? FISMA high?

A I believe in this case FISMA moderate, because it was not deemed high.

Q Why wasn't it deemed high?

A I think you would have to talk to the security folks about that. They do the risk assessment with CCIIO and CMCS. It's a joint business -- you know, it's a risk-based kind of a program that you have to understand the business risk relative to the security controls that are in place.

Q To the best of your knowledge, was an entire security control assessment conducted prior to October 1st?

A Yes.

[Chao Exhibit No. 1
was marked for identification.]

Q Okay. I'm going to introduce Exhibit 1. It's a memo from yourself and James Kerr to Marilyn Tavenner.

Do you recognize this memo?

A Yes.

Q In the memo you wrote, "Due to system readiness issues, the security control assessment was only partly completed. This constitutes a risk that must be accepted and mitigated to support the marketplace day one operations."

What's the security control assessment?

A That's the test that MITRE conducts.

Q Okay. Why is it important?

A Because it tests all the minimum controls that are established by NIST 800-53.

Q What did you mean by the security control assessment was only partly conducted?

A I'm trying to make sure --

Counsel It says "completed" rather than "conducted."

Q Partly completed, thank you.

A It was partially completed because it was -- remember I said it was done in three parts. So I think this was referring to the last part that went prior to the final version that went into production.

Q Who was in charge of conducting the assessment for the Federal marketplace?

A The Chief Information Security Officer.

Q Which is?

A Teresa Fryer.

Q What risk was present from failing to conduct a complete security control assessment?

A I think if you read further on, the background, what this was trying to say was that -- and it goes to your question about, you know, could you have it all in one place, tested end to end? And, you know, my answer was, in a highly ideal sense, yes. But because projects are moving at different rates.

I think the intent of this decision memo was to say that we were rapidly trying to deploy many builds, and it was tested across three timeframes, and that what this was acknowledging was that in the case where you don't have a pristine single environment, all requirements done, everybody in the same environment, that there is an inherent risk with that.

Q So there's a risk from failing to complete the security control assessment?

A Not failing to complete. Not being able to do it in one place all at the same time.

Q But can you flesh out the risk? What is the risk?

A I have to go back to -- well, because it passed all the security controls, I think this was just to say there is some level of risk.

Q Risk of what?

A I have to talk to the CISO, but we were trying to

quantify it in this memo. What we were saying was that the mitigation would be we would have subsequent kind of follow-ups, weekly and monthly security checks.

Q But again, risk of what? Privacy spill? Abrogation of the system? Hacking? What is the risk?

A I think it's risk against any of the controls that we were trying to test against.

Q Risk against any of the controls? Could you elaborate?

A The controls, you know, access, authorization, you know, encrypting of data, secure sessions between browsers when it's supposed to be a secure session. All the controls that needed to be in place.

Q What do those controls guard against?

A Unauthorized access.

Q So the risk of unauthorized access was the risk that you are talking about there?

A That would be one.

Q Okay. What would the others be?

A Just to pick one, maybe not encrypting data in transit and, you know, it's in the clear. So your user ID and password, when it moves in the system, it's in the clear, you could capture it, as opposed to it's encrypted and people can't see it.

Q And why is that a risk?

A Because that then contributes to unauthorized access or the potential for unauthorized access because --

Q So identity theft, for example?

A It's possible, yes.

Q Are there other forms of risks?

A Misrouted data. I'm thinking more on the back end now. Meaning, if you don't have the proper security controls in place, you are issuer A, you are issuer B, we issue security certificates, somehow things got crossed and his file moved to, you know, you and your file moved to him. Right?

Q Okay. What problem does that create if that were to occur?

A That's a PII breach, an incident.

Q Okay. PII is personally identifiable information?

A Correct.

Q So why did you write the memo?

A Why did I write it? I didn't write the, you know, kind of the frame of this. I was given this memo as a, you know, attempt.

This format of how to get to that authority to operate is not something that I created, okay. I think it was a combination of saying, these folks will sign here, pointing to this decision memo that's from Jim and I, so that Marilyn would get a recommendation to sign an ATO. Right?

So when I was given this, it was largely written from a security, you know, what they found in terms of a security assessment, right, but because I'm the lead IT person I needed to

have my fingerprint on this, right, because I am part of it.

I disagreed with something that was in the background. I edited this document. And then it went forth like this.

Q So who primarily drafted it?

A The Chief Information Security Officer.

Q Teresa?

A Fryer, right.

Q So you edited it. What did you edit?

A I think there was a sentence in here. I don't remember exactly what it was, that I thought was inaccurate, so I took it out.

Q Did someone explain the heightened risks of unauthorized access, not encrypting data, identity theft, PII to Ms. Tavenner that would result from not completing the security control assessment?

A I didn't give her that briefing myself, but maybe the CISO did. I'm not sure.

Q Why is Teresa Fryer's name not on the -- as an author on this?

A I think you have to speak to her about that.

Q So you don't know if Ms. Tavenner knew what the heightened risks were from failing to complete the security control assessment before she signed this memo authorizing this decision?

A I think because this is an artifact created through the Chief Information Security Officer in the CIO's signoff process that

she may have been briefed on this, which I was not at the meeting, so I can't speak to that.

Q Okay. So you don't know?

A I don't know.

Q Okay. Who made the decision to proceed with an October 1st launch without a completed security control assessment?

A I don't know.

Q Did you ever discuss the concerns that you had about the heightened risks of failing to complete this assessment with any of your superiors?

A I personally did not feel that the security control assessment was not completed. I believe it was completed. Except framed this way, I think the CISO -- this is my interpretation, right. What the CISO was thinking of was that, going to the example of it needed to all be in one place, all at the same time, no one else touching it. I mean, that almost never happens in any project that I have ever worked on in the 20 years I have been at CMS simply because the schedules don't -- even in a relaxed schedule, you don't have this pristine environment because things are happening and changing every day, right.

So I think what she was trying to address was, it didn't have that ideal condition. But I think that the answer is going to be, we need to look at the security report. The security control assessment report that MITRE produced will address how extensive it was and whether if it was partial or full.

Q So the memo reads, "Due to system readiness issues, the security control assessment was only partly completed." Do you disagree with that?

A I'm saying that it's not characterized correctly. It's not that I disagree with it. I'm saying that because it was done in three parts, I believe the last part fully completed that. But if you only look at the last part, you would say it's partly completed.

Q And do you believe that it constituted a risk that must be accepted and mitigated to support day one operations?

A I think that it would be good practice to be cautious to say, there could be some inherent risk, you know, agreeing to the Chief Information Security Officer that while not being able to have it all in one place -- yes, there's some level of an increased risk.

But from what I could tell -- and I actually didn't get a copy of the final SCA -- I was mainly concerned with whether there were any high findings, which I believe a week later there were no high findings -- that that constituted for me a complete security control assessment.

Q A week later being after October 1st?

A No. A week after the test was completed, which was probably around the second week of September.

Q Okay. So your name is on the memo.

A Uh-huh.

Q The memo that says, the security control assessment is only partly completed.

A Right.

Q So you agree with that?

A As framed by the CISO in whatever -- you know, remember, I did not author this. My name is on it. I edited one section of it. But this was created by the Chief Information Security Officer, right.

Q And the purpose was to get an ATO?

A To address, yes, the need for an ATO.

Q What is an ATO?

A An authority to operate, which under FISMA, every agency has what's called a designated agency official that signs these authority to operate documents to indicate that it's passed some level of security testing, it's passed some evaluation, working in conjunction with business owners, about what risk acceptances exist, and through the collection of the test results and risk acceptance, the ATO is authorized. And it could be authorized for any number of days, right. It could be 90 days. It could be a year. It depends on the situation.

Q Did this result in an ATO being issued, this memo?

A I believe it says here, issue an authority to operate for 6 months to implement the mitigation plan -- and implement a mitigation plan.

Q Is that typical, that an ATO would have those kinds of parameters in them?

A I think the format is not typical. I have not seen this

format before. And I have done quite a few ATOs as a CTO. But I think the temporary nature, you know, for 6 months I have seen before because there may have been -- like in some cases in the past, I have seen systems that had, let's say, 40 medium or moderate, you know, kind of controls that showed some level of risk. Maybe a dozen or so low. And so they are reviewed with the business owners. And they say, well, you know, I think that's, you know, that's good to go, but we need to work on it and to close them, so therefore we issue a 90-day authority to operate. And at the conclusion of 90 days, with a submitted corrective action plan, you close all those out, and then you can get a permanent one.

Q Did all those closeouts occur in this instance with respect to the items referenced in this memo?

A I have to follow up because while I'm saying there were no high findings in the last SCA test, I'm not sure if there were any moderate or low. I need to have the report to kind of see it.

Q Does a provisional ATO of this nature, should it flag additional program risk to the business owner community? Isn't that its purpose?

A I think its purpose is to say, we need to keep a careful watch on it; meaning, the mitigation steps need to be followed.

Q Do you think that proceeding on October 1st without completing the security control assessment was consistent with the highest degree of security and privacy protection?

A Again, I don't know what Marilyn means by high. She is

not a security professional. So I can just say that in the vernacular I use is, you passed the security controls assessment test with no high findings. So we need to, you know --

Q What is the definition of a high finding?

A You know, it's somewhat subjective. It's not consistent. There isn't, you know, you find a smoking gun, and it's only when you find that smoking gun that it constitutes a high finding. I think the security team in discussion about finding a particular exposure in the characteristic of a system that's being deployed -- I'll give you a real-world example.

So if you don't establish a TLS -- see, I can talk about this with you, I know -- if you don't establish a TLS connection, https, you know, secure software connection, that means you are not sitting inside of a private encrypted tunnel between the client machine and the system. So if you are sending, you know, user ID and password in a nonencrypted session, you know, people can intercept that. So that would be a high finding. So that's kind of probably the closest example to a smoking gun I can give you.

So what we would do is, we would make sure that that's corrected so that when you are engaged in that kind of traffic, that you are no longer using port 80, you are going to port 443 to establish an encrypted connection. So that's kind of an example of what a high finding would be and how you could close it.

Q On Wednesday, Secretary Sebelius testified before the Energy and Commerce Committee. Are you familiar with her testimony?

A Yes.

Q Did you brief her prior to her appearance before the committee?

A No.

Q Are you aware of who at CMS briefed her?

A No.

Q At the hearing Secretary Sebelius stated that MITRE did an assessment of the system, gave us a preliminary report, they are in the process of posting a final report. They did not raise flags about going ahead, and the mitigation strategy was put in place.

Are you familiar with the MITRE preliminary report she was referring to?

A I do know that there was a draft. I don't have a copy of it. So I can't say I'm familiar with it.

The most important thing to me was, after the testing was over, I wanted to make sure there were no high findings. So that's kind of what the --

Q I will introduce exhibit number two.

[Chao Exhibit No. 2
was marked for identification.]

Q This is a memo from CMS CIO Tony Trenkle dated September 3rd, titled, "Authorization decision for the Federal facilitated marketplaces system."

Have you seen this document before?

A No. But this looks familiar. This is what a standard

ATO looks like.

Q So the memo contains some findings based on MITRE's security control assessment of the marketplace. The memo identified an open high finding that [redacted]

Counsel Where are you? Do you know where that is in the document?

Q It's on page 205 -- of the attachment, sorry. So probably page 4 of the --

Counsel Page 4?

A 205.

Q It's listed under the finding.

Again, it reads, [redacted]. Do you think that this issue presented a significant risk to the system?

A In my opinion, no, because I think this is actually -- this might be an outdated one. I'm not sure if you actually picked up -- this might be a flaw in the report. Because I was aware of this issue. This issue actually existed during April when we first tested the system in which [redacted] that MITRE had found that that was a problem because it was [redacted]. But I believe that was actually either risk-accepted or cleared up because we weren't doing

that.

Q So you believe that this problem was cleared up by --

A Yes.

Q -- September 3rd, 2013?

A Yes. This could be an error.

Q The memo also identified another open high finding.

A Okay.

Q Was on page 3: [redacted] Do you believe that the presence of [redacted] errors presented a significant risk to the system?

A Yes, I agree with that.

Q When was that corrected?

A I have to look into this. This is the first time I have actually seen this. So don't mind that I'm kind of taking my time reading.

Q So is that a new --

Minority Why don't we give him time to read the whole document.

A Well, I just want to say that I haven't seen this before. And the security program is run between the CIO and the CISO. For the latest status, I think you should probably talk to them about

what's being done about these. And relative to this one, I think I can check and get back to you about whether this was an older finding that just kind of carried forward. It may not necessarily be there. I'm not even copied on this.

Q So it's dated September 3rd, which is, you know --

A Right. Right around the time --

Q -- couple weeks prior to the launch. Why don't you take a couple minutes and review it and then just answer our questions to the best of your knowledge.

A Well, I'm not even copied on this, so I don't -- I don't have any basis for answering your questions about this document because I wasn't part of creating it. I wasn't copied on it.

Q But you understand what the term "functional testing process" is, correct?

A Again, I think that there are details behind these descriptions that I would feel more comfortable if I had the CISO and the MITRE test team here and --

Q No, I understand. But the term "functional testing process," that's a term of art, is it not? I mean, you know what this alludes to, the topic of this memo? You understand these words, correct?

Minority This is a memo that you are showing him now for the first time that he's never actually --

Q I'm sorry, Ms. Grooms. We have an hour. Then you have an hour.

Minority I know. Could we just let him read the whole memo before we ask him any more questions about it?

Q We just gave him an opportunity to do that. But I ask that you stop interrupting.

A You are familiar with the concepts in this memo given your position as Chief Information Officer, Deputy Chief Information Officer handling the Affordable Care Act, correct?

A I need to see the report because this is not specific. I mean, the term, [redacted] that's a mouthful. What's the example of that happening?

Counsel I think he just hasn't seen it. So maybe it's better for him to follow up.

Q Do you find it surprising that you haven't seen this before?

A Yeah. I probably should have been copied on it.

Q Because, I mean, it appears that this is the results of MITRE's security test of the system.

A Well, why I'm surprised is that the CISO had me do this, file this process, but don't copy me on the ATO letter. I mean, wouldn't you be surprised if you were me?

Q Yeah.

Q I would.

Q Now, the second column says, [redacted]

[redacted] Do you see that language in the second column under fining description? On page 3 of 5, second column, finding description, second sentence.

A I don't even know how that can be true because on September 3rd [redacted]

Q But that's not my question. My question is, the statement, [redacted] is that, to your understanding as a systems professional, is that supposition correct?

A It's highly speculative because it may.

Q That's not my question. My question is --

A I'm saying the word "may." I'm saying the word "may" is highly speculative because on September 3rd [redacted]. So that's why I find it confusing to read this, because [redacted]

Q But in your experience have you ever seen a circumstance where [redacted]? Have you ever seen that circumstance occur?

A I would need the specifics. In my experience that's a very generalized, speculative statement. I need to see the results.

Q So it's your testimony that you have never seen or never experienced a situation in any large IT development or deployment effort where [redacted] --

A No. You are putting words in my mouth. I am saying --

Q That's what I do. I'm a lawyer. It's a joke.

Minority That's not what they do.

Minority That's not what lawyers do.

Q Tongue in cheek.

A I will say --

Counsel He is just saying he is uncomfortable speculating about the underlying rationale for a document he hasn't seen.

Q Who is the Chief Information Officer and Director of the Office of Information Services?

A Tony Trenkle.

Q Are you surprised that this memo is from him and it appears to be about major issues involved with the Affordable Care Act implementation as it deals with www.healthcare.gov --

A Yes.

Q -- that you didn't see this memo until we handed it to you today?

A Yes.

Q Who's the Director of the Consortium for Medicare Health Plans Operations?

A That's Jim Kerr.

Q Who's the Acting Deputy Director for Operations, the

Center for Consumer Information?

A That's Jim Kerr. He is on a detail from the New York regional consortia.

Q And Jim Kerr is listed --

A Right.

Q -- on the memo to Marilyn Tavenner on September 27st.

A Right. Uh-huh.

Q So you are surprised that he never -- either Mr. Trenkle or Mr. Kerr ever shared this document with you?

A No.

Q You are surprised?

A I'm surprised.

Q Okay. I think we'll move off this document for now.

What was the role of the CMS CISO, Teresa Fryer, in the decision to certify the exchange?

A As a matter of protocol and procedure, in the Federal Government the Chief Information Security Officer is in charge of the program and operations of, you know, the agency's kind of information systems security program.

****

Q I want to turn your attention back to Exhibit 2. Okay, so this is the memo from September 3rd from Mr. Trenkle to Mr. Kerr. The second paragraph in the memo says, "On August 8, 2013, you

certified the controls for the system and submitted along with your certification the other required documentation necessary to obtain an Authorization to Operate."

The way this is written, the "you" would be James Kerr. Is that your understanding, that James Kerr certified the controls for the system?

A I'm not familiar with that. It reads kind of odd to me somehow.

Q Okay.

On the second page, it says, "The attachment provides information on requirements not met, as well as corrective actions needed to bring them into compliance. The actions set forth in the attachment must be entered into the approved CMS Plan of Action and Milestones tracking tool no later than 30 days from the date of this memorandum, and the action items addressed no later than the designated completion dates."

Are you familiar with the CMS Plan of Action and Milestones?

A I understand the process. I don't understand -- I don't know exactly what was entered for this.

Q The individuals CC'ed on this memo, are you familiar with these individuals?

A Yes. They are all in -- I have never met Jessica before, but everybody else I've met. They are OIS employees.

Q Have you worked with any of these individuals closely on your work related to the Affordable Care Act?

A Mark Oh.

Q Mark Oh?

A Uh-huh.

Q Any of the others?

A Darrin Lyles a little bit. Probably those two more than anybody else.

Q What's the nature of your relationship with Mr. Oh?

A He is, like, the technical lead, I mentioned earlier, for the marketplace program.

Q Do any of these individuals report to you?

A Mark does. Darrin reports to Monique Outerbridge and Kirk Grothe in that consumer information insurance systems group, the "CIISG" you see there.

Q Uh-huh. So do you find it unusual that there is a memo from people that you report to, people that report to you are CC'ed, and you aren't aware of it?

A It is kind of strange. Maybe it's an oversight. I don't know.

Q So the next page, the first page of the attachment, says "CMS Sensitive Information -- Requires Special Handling." Have you seen that before?

A You mean the format of this document?

Q The top of the page, "CMS Sensitive Information -- Requires Special Handling."

A Well, I've seen ATO forms. Yeah, I think this is

boilerplate what they put.

Q The "Sensitive Information -- Requires Special Handling"?

A Uh-huh.

Q Okay.

There are several findings issued here. And since this report was, or this memo, the date is September 3rd, my question is going to be which of these findings you were aware of as existing as of September 3rd.

So the first finding is the [redacted] Were you aware of that finding existing as of September 3rd?

A No.

Q The second finding, "FFM has an open high finding: [redacted] were you aware of that finding as of September 3rd?

A No.

Q The third finding, "[redacted] controls are described in [redacted] as 'Not Satisfied,'" were you aware of that finding as of September 3rd?

A No.

Q The fourth finding, "[redacted]" were you aware of that

finding as of September 3rd?

A No.

Q The fifth finding, "[redacted]," were you aware of that finding as of September 3rd?

A No.

Q The sixth finding, "[redacted]" were you aware of that finding as of September 3rd?

A No.

Q Did any of these individuals subsequent to September 3rd discuss any of these findings with you?

A No.

Q Okay. Do you expect that they should have?

A Not necessarily. I think the -- each major project is assigned an information systems security officer, which that person -- like, in this case, it's Darrin Lyles; you see the ISSO designation -- that their job is to make sure that, between the contractors, the business owners, and the security team, because they are representative of the security team, are working together to make sure that things do go to CFACTS, they are documented, and they are working the Plan of Action and Milestones, and that, you know, progress is being made in addressing these deficiencies.

Q Is there any reason you can of that you were excluded from receiving this information?

A No.

Q On September 27th, you issued the memorandum that we've discussed to Marilyn Tavenner, along with James Kerr?

A Uh-huh.

Q The memo stated, again, that, "From a security perspective, the aspects of the system that were not tested due to the ongoing development exposed a high level of uncertainty that can be deemed as a high risk for FFM. Although throughout the three rounds of SCA testing all the security controls have been tested on different versions of the system, the security contractor has not been able to test all the security controls in one complete version of the system."

Should you have known the issues identified in the September 3rd memo before you put your name on the September 27th memo to Ms. Tavenner?

A I would think so.

Q How do you feel about being unaware of these issues prior to putting your name on that memo on September 27th?

A I'm surprised. And I probably -- with that knowledge, I would have at least acknowledged what those findings were in this risk assessment.

Q Are you just surprised or are you angered that you didn't know?

A No, I'm not angry. I got many more things in life to be angry about. I'm not angry about this.

Q But you take the security of the FFM very seriously,

right?

A Correct.

Q And you were being excluded from finding out about significant problems with security.

A It is disturbing. I mean, I don't deny that this is, kind of, a fairly nonstandard way to document a decision to make a recommendation to proceed in ATO. I have not ever since -- I began CTO of CMS in 2007, in late 2007, and I was part of the process for, you know, 3 years to sign off on these. This kind of format I have never seen before, so, I mean -- but I follow what I --

Q So you were presented with the outline of that memo and asked to put your name on it without knowing the full scope of issues underlying the memo?

A To the best of my knowledge at that point in time, this came pretty close to what I understood, that security testing had occurred, not in one environment but all controls were covered across three tests, and that there were no high findings. That's my understanding at that time.

Q As of what dates were you of the belief that there were no high findings?

A Let's see, very -- what's the date on this?

Q The memo is the 27th.

A Yeah, it was not the 27th. I have to double-check my calendar, but it was when I was waiting for the security team, the testing team, to be finished at CGI in Herndon. I was actually

onsite. And it was a Friday in early September, I think. But I have to check my calendar to see.

Because, you know, I was interested. I'm like, okay, guys, did we pass or, you know, do we have any problems? And the report out from Darrin Lyles and Tom Shankweiler, who is another ISSO that works on this project, said we had no high findings.

Q Does this suggest that the lines of communication within the organization were not working properly?

A It's a good possibility.

Q Does it reflect on systemic issues with the way the program was operated or organized?

A I don't necessarily think that that, kind of, translates immediately to that. I think, in this particular case, yes, the documentation and my recollection seems to point to, you know, kind of, a failure to communicate.

Q You said the development of the memo was highly unusual that went to Ms. Tavenner.

A I said it was unusual. I have never seen it this way before.

Q Well, how does it usually work with memos that you're going to be --

A It results in a big, thick binder of all the security testing results, all the findings, a summary page, and then an authority to operate, with sometimes an appendix that says, if there are, you know, 15 findings, it summarized them in the appendix so

you don't have to dig into the big documentation.

I'm used to seeing that big binder come across my desk. And, as a CTO, I was part of the signatory process, right? I would recommend or not recommend it. And, ultimately, it would be signed by the CIO, who is the designated agency official.

So I'm used to seeing, kind of, the package in that manner. I was unfamiliar with this.

Q Would that package reflect a full vetting and explanation of the various findings in a way that you could look at and ascertain?

A Yes. Because if you want to dig into the details, because you have the ATO letter, you have a summary of the findings, just like this, you have an even better summary of the findings generally in an attachment, and then you can actually see the test results that are, kind of, inside the binder.

Q When you said "something like this," can you be specific what you're referring to?

A It's typically a -- it's called a --

Q You're referring to the September 3rd --

A This is just a piece of it. There is a probably a binder this thick that goes with this, okay?

Q So when this came in and you saw that this shortcut had occurred, what was your reaction?

A I said to myself, they must be trying to -- because it's such a large program -- to try to get more signatures on it instead

of just one person. Right?

Q For the record, when you say "this thick," what does that mean?

A It's a big binder, maybe 3, 4 inches thick. Large programs, sometimes we have two or three binders. And it represents all the test results, all the documentation that is generated through the security testing that has occurred throughout, you know, kind of, the date, the remaining -- you know, whenever they started security testing and whenever we went into production.

The documentation would reflect what tests were being done, what findings were discovered. Sometimes, you know, the POA end plan is also in there that says, by this date we will fix these things.

Q I mean, we have heard that the setup for the Affordable Care Act is one of the most complicated things that the Federal Government has ever tried to set up. So you would have expected multiple binders when you were looking through this, correct?

A Well, you know, I'm not the CTO anymore, and, you know, while I'm the deputy CIO, I'm largely focused on the marketplace project. So I was not necessarily, you know, taken aback that our acting CTO could have very well been reviewing the much more extensive documentation.

Q Who is the acting CTO?

A George Linares.

Q Did you question why you weren't presented with, sort

of, the full results of the testing?

A No. No. No.

Q When this shortcut occurred, did it raise any red flags with you?

A I wouldn't say red flags. I was just unfamiliar with it.

Q Were there other instances in your program activity where you were blindsided like you were in this instance?

A I wouldn't call it blindsided. I --

Q What would you call it?

A An omission. I don't want to think the worst of people. I mean, it's very easy to omit people on these things. And so, you know, I don't consider it blindsided. I just figured they had inadvertently omitted me.

Q But you weren't just omitted from the memo; you were also omitted from the information contained in the memo.

A The information contained in the memo, like I said, I think the assumption I would make now is that the CTO is in a review process, so he would have looked at it.

Q Let me go back to Exhibit 7. I think it's Exhibit 7, the health insurance marketplace preflight checklist.

Counsel Maybe it's 8? Was there an 8?

Q Six.

Q Would you turn to page 32?

A Page 32 here?

Q Yes. So we established that the date on this packet is

September 17th. This is the security checklist?

A Uh-huh.

Q And under the system, it lists "FFM." And under the category residual risks, it has "too high." Where are those high risks that were remaining as of September 17th?

A I would have to look at what it says, the notes, the certification form for details, which -- is it part of this?

Q We couldn't find it. So you're unaware of what the two high risks are in the FFM as of September 17th?

A Correct.

Q So the September 3rd memo lists the two high risks?

A Yeah, there -- I think that -- if you recall, I said that I was onsite, and I was, you know, very anxious, talking to the security team about whether there are any findings, you know, during that last test. And, you know, if you look at the FFM, what I recall is what the team told me, is that there were no high findings.

I think that -- that's SCA testing, right? We have a security operations center, what we call an exchange security operations center, that monitors the system activities on a day-to-day basis. They opened some, like, tickets on whether if they see a certain risk. They have a tool, Trend Micro, that is running in the system all the time, so when it triggers, like, some event, they also log certain risks that are captured by that tool.

I think this might be part of these other -- because it doesn't

match up. If there are no high findings from the SCA and the ATOs, you know, because it's, yes, it's been conducted, yes, it got an ATO, no high findings, then --

Q No high findings remediated?

A Well, no need to because there are no high findings, right? I don't know. I need to see the --

Q No high findings were mediated.

A Yeah, I need to see the certification form. Because I recall that in the conversation that some folks were mixing in our security operations center monitoring with the SCA results, which you typically don't do that either.

Q Okay. So there's two possibilities. Because you said that sometime by early September that there were no more high findings.

A Uh-huh.

Q So either that's the case and this document is incorrect or what you thought in early September was incorrect and the document is correct, that there were still high findings as of September 27th.

A Yeah, we need to confirm that. I agree.

Q Does that suggest some confusion in the reporting and tracking of these high-risk elements?

A I think so.