BGIN Meeting Report

Date: TBD
Location: Virtual Meeting

Executive Summary

The meeting focused on several key areas aimed at enhancing security within blockchain and crypto ecosystems. The primary topics included mapping existing security frameworks and standards to avoid redundancy while addressing unique crypto-native risks. The group discussed potential collaborations with organizations such as NORS, 3GPP, and the Blockchain Security Standards Consortium (BSSC) to ensure a comprehensive approach. Sandra shared her organization's multi-layer cyber security strategy, which includes detailed risk frameworks and mitigation techniques tailored for regulated financial institutions.

Additionally, the meeting highlighted the upcoming NIST workshop on April 16th, where the group expressed interest in contributing to the agenda. The focus will be on structuring documentation and utilizing frameworks like the National Vulnerability Database (NVD) to define Common Vulnerabilities and Exposures (CVEs). This effort aims to systematically address both threats and vulnerabilities within the blockchain and crypto sectors, ensuring a more secure and resilient ecosystem.

Key Discussion Points

- **Mapping Existing Standards**: The group aims to map existing security frameworks and standards to avoid duplication of effort.
- **Crypto-Native Risks**: Focus on unique risks specific to blockchain and crypto ecosystems, such as account takeovers and scams.
- **Collaborations**: Potential collaborations with organizations like NORS, 3GPP, and BSSC are discussed.
- **Sandra's Organization**: A multi-layer approach to cyber security for regulated financial institutions, including risk frameworks and mitigants.
- **NIST Workshop**: Interest in contributing to the agenda of the upcoming NIST workshop on April 16th, particularly in structuring documentation using frameworks like the NVD.

Action Items and Next Steps

1. **Reach Out to BSSC**: Initiate contact with BSSC to explore collaboration opportunities.

2. **Review JFSA/Japan Work**: Look into the work done by JFSA and other Japanese organizations to ensure alignment.
3. **NIST Workshop Preparation**: Prepare an agenda for the NIST workshop, focusing on structuring documentation and using frameworks like the NVD.
4. **Remote Sessions**: Schedule remote sessions to start laying the groundwork for mapping existing standards and frameworks.

Next Steps

- The group will break for lunch and reconvene in one hour.
- After the break, there will be a presentation from GFSA followed by a session on key management.
- The team will continue to work on mapping existing security frameworks and preparing for the NIST workshop.

Detailed Session Summary

The meeting begins with a discussion on the importance of mapping existing security frameworks and standards, particularly in the context of blockchain and crypto ecosystems. The group aims to avoid reinventing the wheel while ensuring that unique crypto-native risks are addressed. They discuss potential collaborations with organizations like NORS, 3GPP, and BSSC (Blockchain Security Standards Consortium). Sandra shares her organization's multi-layer approach to cyber security, which includes risk frameworks and mitigations for regulated financial institutions.

The discussion then shifts to the upcoming NIST workshop on April 16th. The group expresses interest in contributing to the agenda of this workshop, particularly in structuring documentation and using frameworks like the National Vulnerability Database (NVD) to define CVEs and discuss both threats and vulnerabilities.

The meeting focused on several key areas aimed at enhancing security within blockchain and crypto ecosystems. The primary topics included mapping existing security frameworks and standards to avoid redundancy while addressing unique crypto-native risks. The group discussed potential collaborations with organizations such as NORS, 3GPP, and the Blockchain Security Standards Consortium (BSSC) to ensure a comprehensive approach. Sandra shared her organization's multi-layer cyber security strategy, which includes detailed risk frameworks and mitigation techniques tailored for regulated financial institutions.

Additionally, the meeting highlighted the upcoming NIST workshop on April 16th, where the group expressed interest in contributing to the agenda. The focus will be on structuring documentation and utilizing frameworks like the National Vulnerability Database (NVD) to define Common Vulnerabilities and Exposures (CVEs). This effort aims to systematically address both threats and vulnerabilities within the blockchain and crypto sectors, ensuring a more secure and resilient ecosystem.

Appendix: Full Meeting Transcript (Anonymized)

28.6 --> 30.0: This is a meeting transcript.
58.6 --> 60.0: This is a meeting transcript.
88.4 --> 90.0: This is a meeting transcript.
90.0 --> 90.8: It is an online session.
90.8 --> 90.9: It is an online session.
90.9 --> 90.9: It is an online session.
90.9 --> 93.1: If there is anyone online,
93.2 --> 93.9: If there is anyone online,
93.9 --> 100.1: it took us a bit more time to reach the area of the coffee.
103.2 --> 104.7: Just to keep it short,
104.8 --> 108.1: we are going to start the second session of this morning.
108.4 --> 109.1: So please, everyone,
109.4 --> 111.0: we are going to start.
112.2 --> 115.1: This session is on governance of supply chain,
115.2 --> 117.0: or let's say security of supply chain.
117.0 --> 117.8: supply chain management.
121.2 --> 124.0: We are going to start, as I said.
124.3 --> 124.7: We are going to start, as I said.
124.7 --> 127.9: We will start with a first presentation
128.7 --> 129.4: from
131.0 --> 132.6: JP Crypto Isaac
134.0 --> 134.7: representative
135.5 --> 137.0: on what they are working on currently.
137.0 --> 138.8: on what they are working on currently.
139.5 --> 141.8: So please, take a seat everyone, and let's start.
148.7 --> 150.9: Speak loud to get people to come.
152.3 --> 153.6: Speak loud to get people to come.
153.6 --> 154.5: Hello, everyone.
155.0 --> 157.2: This is Sasaki from JP Crypto Isaac.
157.9 --> 160.1: Today, I would like to share
160.1 --> 162.0: the third-party guidance
162.0 --> 163.4: built by
163.4 --> 165.8: JP Crypto Isaac in this
165.8 --> 166.2: January.
167.8 --> 169.6: Before explaining this
169.6 --> 171.8: guideline, let me share
171.8 --> 173.5: JP Crypto Isaac again.
174.3 --> 175.9: Currently, JP Crypto Isaac
175.9 --> 177.1: has
180.6 --> 182.0: 14 is about

182.0 --> 182.5: the
182.5 --> 184.4: cryptocurrency company
184.4 --> 185.5: licensed by
185.5 --> 186.4: FSA,
187.5 --> 188.9: and support members
188.9 --> 189.8: is about
190.8 --> 193.2: 10, and so on.
193.6 --> 195.2: We are just
195.2 --> 196.8: proceeding many things,
197.1 --> 198.7: including sharing information,
199.2 --> 200.6: guideline, and so on.
200.6 --> 202.7: Recently,
203.6 --> 204.6: in Japan,
205.2 --> 206.6: one key
207.3 --> 208.6: point is
208.6 --> 210.8: three pillars of defense.
212.0 --> 212.5: Here,
212.7 --> 214.4: three is
214.4 --> 216.6: self-help,
221.9 --> 223.3: which is because
223.3 --> 224.8: cryptocurrency companies
224.8 --> 226.2: have to cope
226.2 --> 228.7: with many incidents by
228.7 --> 229.0: themselves.
230.2 --> 232.2: This is one key factor.
232.9 --> 234.4: Another is from the government
234.4 --> 236.8: support by
236.8 --> 237.6: JFSA.
238.5 --> 240.7: Today's topic is mutual
240.7 --> 242.7: aid, which is a Japanese
242.7 --> 243.6: word, kyojo.
244.9 --> 246.2: JP Crypto Isaac
246.2 --> 248.2: have to have this role
248.7 --> 249.9: to cooperate with
249.9 --> 252.5: JP Crypto Currency companies
252.5 --> 254.3: with JBCA.
255.5 --> 257.3: Let me
257.3 --> 258.3: share the situation
258.9 --> 260.3: of the
262.0 --> 262.6: theft
262.6 --> 264.6: incident, asset incident,
264.9 --> 267.0: recently from the year.
268.0 --> 268.8: We
268.8 --> 269.7: categorize
270.3 --> 272.3: three patterns.
273.6 --> 274.5: One is
274.5 --> 276.3: from sharp

276.3 --> 277.7: 1 to 4,
278.3 --> 280.8: next is sharp 5 to 8,
281.1 --> 283.3: and lastly is 9 to 13.
283.3 --> 285.1: From 1
285.1 --> 287.2: to 4, the attack
287.2 --> 288.5: method was
289.3 --> 290.0: hot wallet.
290.7 --> 293.1: This is, for example, done by
293.1 --> 294.1: Mt. Gox,
295.1 --> 296.7: Coincheck, and so on.
297.0 --> 298.7: This was a major attack
298.7 --> 299.4: in Japan.
300.5 --> 303.0: Next is, for example, smart
303.0 --> 304.1: contract attacks.
304.9 --> 305.4: Recently,
306.1 --> 308.5: we detected many
309.3 --> 310.7: incidents by supply
310.7 --> 311.2: chain,
311.9 --> 312.9: for example,
314.2 --> 315.8: Ginko-san, and so on.
316.4 --> 317.6: I think
318.7 --> 320.5: the attack method
320.5 --> 321.8: is just changing,
322.5 --> 324.1: and we have to cope
324.1 --> 325.9: with many attacks method.
328.6 --> 330.3: Let me share the
330.3 --> 331.7: supply chain threats.
332.9 --> 333.8: Attackers
334.7 --> 336.3: attacked the third-party vendor
336.3 --> 338.0: rather than
338.0 --> 340.0: the crypto exchange company
340.0 --> 342.3: because the third-party
342.3 --> 343.7: vendor has
343.7 --> 346.1: a potential or power
346.1 --> 347.6: to control
347.6 --> 348.7: the wallet.
349.6 --> 351.1: I think the attackers
352.0 --> 354.4: found it useful
354.4 --> 355.7: for them
355.7 --> 358.0: to attack the third-party
358.0 --> 360.1: vendor rather than the crypto exchange company
360.1 --> 362.1: because the crypto exchange
362.1 --> 362.8: company
362.8 --> 366.0: has many things
366.0 --> 367.6: to protect
367.6 --> 369.1: by themselves
370.0 --> 371.5: by receiving

371.5 --> 372.6: many threats.
373.9 --> 375.6: Here is the left
375.6 --> 377.6: figure. Supply chain attack
377.6 --> 379.8: is here. Lastly,
380.3 --> 381.6: customer asset
381.6 --> 383.0: was stolen.
384.5 --> 385.8: The problem is
385.8 --> 387.4: because attackers
388.0 --> 389.7: target weakest links
389.7 --> 390.9: in supply chain.
391.7 --> 394.0: Recent incidents
394.0 --> 395.8: occurred in supply chain
395.8 --> 397.1: and we have to
398.0 --> 399.6: try to protect
399.6 --> 400.9: this field.
401.5 --> 403.7: This is today's main topic.
406.0 --> 407.8: Here is an image of
407.8 --> 409.7: the supply chain
409.7 --> 411.6: in permissionless blockchain-based
411.6 --> 412.2: systems.
414.0 --> 415.5: The top side is BASP
415.5 --> 417.7: or stablecoin issuers.
418.5 --> 419.1: Sometimes,
419.6 --> 421.9: BASP stablecoin issuers
421.9 --> 423.5: rely on wallet
423.5 --> 425.9: vendors like Japanese
425.9 --> 427.6: wallet vendors or overseas
427.6 --> 428.4: wallet vendors.
429.9 --> 431.7: Japanese wallet vendors
431.7 --> 434.2: and overseas wallet vendors
434.2 --> 435.3: use
435.9 --> 437.8: cloud infrastructure like
437.8 --> 439.6: Amazon,
439.7 --> 441.3: AWS, Azure,
441.9 --> 442.6: and GCP.
444.1 --> 444.8: Lastly,
446.9 --> 448.6: by using
448.6 --> 449.6: the cloud infrastructure,
449.6 --> 451.2: wallets are
451.2 --> 453.3: withdrawing to
453.3 --> 454.0: blockchain.
455.3 --> 457.7: Our topic is
457.7 --> 459.4: the wallet vendors.
460.1 --> 461.4: This is today's major
461.4 --> 462.1: topic.
463.8 --> 465.6: J.P. Krutoizak
465.6 --> 466.9: developed the

466.9 --> 469.9: good practices based on
469.9 --> 471.6: FISC framework.
472.6 --> 473.5: The background is
473.5 --> 475.3: because, as I explained to
475.3 --> 477.2: this, security
477.2 --> 479.1: incident in Japan
479.1 --> 481.2: traced to supply chain
481.2 --> 481.8: vulnerabilities.
483.9 --> 485.6: Our focus
485.6 --> 487.6: is here, and we
487.6 --> 489.6: developed the good practices
489.6 --> 490.8: later.
492.0 --> 493.3: In response,
493.9 --> 494.9: Japan is
494.9 --> 497.1: proactive in establishing the
497.1 --> 499.6: industry standards for supply chain security,
500.3 --> 501.2: and J.P. Krutoizak
502.0 --> 503.5: has utilized
503.5 --> 504.5: these guidelines.
504.5 --> 506.4: This was
506.4 --> 508.6: published by September 2025
508.6 --> 510.7: internally.
511.8 --> 513.3: J.P. Krutoizak
513.3 --> 514.6: members have
514.6 --> 516.6: used this guideline
516.6 --> 518.8: to protect by themselves.
520.9 --> 522.6: What is FISC?
523.0 --> 524.5: FISC is
524.5 --> 526.4: Japan's financial IT
526.4 --> 528.0: security authorities,
528.6 --> 530.9: and this was established by
530.9 --> 532.8: 1984.
532.8 --> 534.8: I think this is
534.8 --> 537.1: a historical documentation
537.1 --> 537.9: and so on.
538.7 --> 540.0: In Japan,
540.6 --> 542.7: for example, banks, insurance,
542.9 --> 544.2: securities, and many
544.8 --> 546.1: finance services
546.8 --> 548.3: used this
548.3 --> 550.7: FISC because
550.7 --> 552.3: FISC teaches
552.3 --> 554.7: many things
554.7 --> 556.2: to companies,
556.6 --> 558.6: and we sometimes rely on
558.6 --> 559.3: this guideline.
560.5 --> 562.3: J.P. Krutoizak

562.3 --> 564.1: utilized FISC
564.1 --> 564.9: and so on.
566.2 --> 567.8: Here is an image
567.8 --> 569.8: of the positioning
569.8 --> 572.0: of J.P. Krutoizak guidance.
573.4 --> 575.5: Please see the
575.5 --> 576.8: top page.
577.5 --> 579.3: JSA, FSA,
579.8 --> 581.3: and JBCA, and FISC
581.9 --> 583.9: are the guidelines for me,
584.2 --> 585.1: J.P. Krutoizak.
585.6 --> 587.3: J.P. Krutoizak have copied
587.4 --> 589.8: or mimicked these guidelines
589.8 --> 591.7: and write
591.7 --> 593.4: the functional situation
594.0 --> 595.4: to vendors,
595.6 --> 597.6: how to use, how to protect
597.6 --> 599.4: some things. So this is
599.4 --> 601.5: a good practice collection.
603.4 --> 605.3: What is clever about
605.3 --> 606.5: these guidelines?
607.3 --> 608.9: One is the controls
609.4 --> 611.1: for cloud services.
612.0 --> 612.8: Because
613.4 --> 615.8: a cryptocurrency company
615.8 --> 617.6: and wallet vendors have
617.6 --> 619.6: to understand how to
619.6 --> 621.0: use the cloud.
621.4 --> 623.0: This is a really important thing.
623.9 --> 624.8: But currently,
625.1 --> 627.5: some documents write
627.5 --> 628.3: the abstract,
629.8 --> 631.2: but J.P. Krutoizak documents
631.2 --> 633.7: write details, so how to utilize,
633.9 --> 635.9: how to set, settings,
636.1 --> 636.5: and so on.
637.3 --> 639.6: Next is the controls for wallet system
639.6 --> 641.3: vendors because
642.2 --> 643.0: sometimes
643.0 --> 645.0: J.P. Krutoizak companies
645.0 --> 646.9: rely on wallet vendors
646.9 --> 649.2: and have to
649.2 --> 650.8: control more
650.8 --> 652.7: and more because
652.7 --> 654.4: some issues
655.0 --> 656.8: is occurred by
656.8 --> 658.7: wallet vendors and cryptocurrency

658.7 --> 660.9: companies have to understand
660.9 --> 662.4: this situation.
664.5 --> 666.4: Yes, so
667.0 --> 668.8: this is summary of this
668.8 --> 670.4: category guideline.
670.4 --> 672.0: We focus
672.0 --> 674.3: on the wallet service vendors
674.3 --> 675.7: center
676.4 --> 678.4: point. For example, the
678.4 --> 680.7: direct contractual
680.7 --> 681.8: relationship
682.4 --> 683.9: or how to
684.4 --> 686.3: utilize cloud and so on.
689.1 --> 690.6: I will share
690.6 --> 692.6: the guidelines image later,
693.1 --> 694.1: but here is
694.1 --> 694.8: the structure.
695.7 --> 698.4: We have the main document
698.4 --> 699.8: which is
701.5 --> 702.4: good
702.4 --> 703.1: protection
704.2 --> 706.6: on third-party risk management
706.6 --> 708.4: and we have three
708.4 --> 710.4: appendices. One is the MOU
710.4 --> 712.1: template. This is
712.1 --> 714.5: between the wallet vendors
714.5 --> 716.8: and cryptocurrency companies because
716.8 --> 718.6: cryptocurrency companies sometimes
718.6 --> 720.4: don't know how to
720.4 --> 722.0: contract the wallet vendors.
722.4 --> 724.1: This is one sample
724.1 --> 726.2: to contract
726.2 --> 728.0: with vendor,
728.3 --> 730.2: wallet vendor. Next is
730.2 --> 732.0: architecture program and last
732.0 --> 733.9: so appendix 3 is most
733.9 --> 735.6: important file.
736.1 --> 738.2: This is a checklist. So because
738.2 --> 740.1: this checklist concludes
740.1 --> 741.5: about 100
742.2 --> 743.7: checklists, but
743.7 --> 745.7: probably cryptocurrency
745.7 --> 748.4: companies can check
748.4 --> 750.0: this by using
750.0 --> 752.1: this checklist. After that
752.1 --> 754.1: probably the security level
754.1 --> 755.5: will be up.

757.1 --> 758.1: I will change the
758.1 --> 758.5: document.
766.0 --> 767.4: Here is
768.1 --> 770.4: the main document, third-party
770.4 --> 771.2: risk management.
772.1 --> 773.9: This is a story
773.9 --> 775.1: written by
776.1 --> 776.5: Hirashita-san.
778.4 --> 779.6: Here is the huge
779.6 --> 781.7: documentation, but
781.7 --> 783.3: this concept is
783.3 --> 785.1: how to
785.7 --> 787.1: utilize, how to use,
787.4 --> 789.4: how to integrate
789.4 --> 790.3: something.
791.2 --> 793.7: Sometimes members of cryptocurrency
793.7 --> 795.7: companies don't understand
795.7 --> 797.6: the detail about
797.6 --> 799.1: the security and so on.
799.6 --> 801.8: This is one sample
801.8 --> 803.2: how to proceed
803.7 --> 805.5: this. I think this is
805.5 --> 807.5: really important documentation.
808.7 --> 809.5: I think
809.5 --> 811.5: so company had better
811.5 --> 813.4: read this according to this
813.4 --> 813.8: guideline.
816.1 --> 817.2: Next is
817.2 --> 819.1: here is the MOU
819.1 --> 821.4: so the contract sample.
822.2 --> 822.9: So probably
823.5 --> 824.1: it's really
825.3 --> 827.1: some conditions,
827.4 --> 829.4: but it's important thing to
829.4 --> 831.4: understand the importance
831.4 --> 833.3: of difficulties between
833.3 --> 835.1: the contract of supply chain
835.1 --> 837.2: and cryptocurrency company.
839.5 --> 841.4: The last story is here.
842.0 --> 842.8: Sorry, this is
843.5 --> 845.3: small font size, but
845.3 --> 846.9: I think it's
849.2 --> 851.1: so this is a really
851.1 --> 853.7: important checklist because
853.7 --> 855.2: for example,
855.5 --> 857.5: let me share
857.5 --> 859.0: one point.

859.5 --> 860.4: For example, this is
861.5 --> 863.1: 20 checklist number
863.1 --> 864.7: so security assessment.
865.8 --> 867.2: So we
867.2 --> 869.0: recommend how
869.0 --> 871.0: to use DMZ
871.0 --> 872.7: design and so on.
873.6 --> 874.7: And here
874.7 --> 877.0: we write some
877.0 --> 878.8: recommendation to
878.8 --> 880.1: customers
881.2 --> 882.7: how to check
882.7 --> 884.8: or how to contract this.
885.3 --> 886.7: So how to build this.
887.5 --> 889.1: So I think this
889.1 --> 890.8: is a bit of huge
890.8 --> 892.5: checklist, but
893.2 --> 895.1: I think this is probably
895.1 --> 897.2: useful for cryptocurrency company.
898.4 --> 899.1: And today
899.1 --> 900.9: so this
900.9 --> 903.1: documentation was just
903.1 --> 904.8: built and published
904.8 --> 907.2: internally. So today
907.2 --> 909.1: so this is a first
909.1 --> 911.1: step how to
911.1 --> 912.8: proceed in begin
912.8 --> 915.1: and so on. That is
915.1 --> 916.7: from me. Thank you.
928.4 --> 929.4: Thank you.
929.5 --> 930.1: Any question?
931.2 --> 931.6: Comments?
938.2 --> 940.0: I like the fact that
940.0 --> 942.0: there's initiatives to make this happen.
942.9 --> 944.1: It most specifically
944.1 --> 945.7: as a Japanese citizen and
947.1 --> 948.1: working as
948.1 --> 949.3: an integrator for
949.3 --> 952.0: various security solutions and
952.0 --> 953.8: seeing this framework. I
953.8 --> 955.9: hope to also personally add to this
955.9 --> 956.4: as well.
958.3 --> 959.8: Yes, I do agree
959.8 --> 961.4: that a lot of the crypto companies
963.2 --> 963.8: don't
963.8 --> 965.6: get the security or understand the security
965.6 --> 967.8: ramifications. And I like the fact that you did

967.8 --> 969.9: highlight the evolution
969.9 --> 972.1: between hot wallets
972.1 --> 974.1: to then eventually cold wallets
974.1 --> 975.8: and the business and
975.8 --> 977.7: how mostly the regulatory
977.7 --> 979.8: aspects and compliance is forcing
979.8 --> 981.8: this change to happen. And
981.8 --> 983.6: I think the activities
983.6 --> 985.0: with the Japan
986.3 --> 987.4: Virtual Currency
988.1 --> 988.6: Association.
989.6 --> 991.1: I forget the acronym.
991.6 --> 993.5: But I do hope to be a part of that and help
993.5 --> 995.6: drive these endeavors and be an
995.6 --> 996.9: active voice around that.
998.0 --> 999.6: Because it is something that needs
999.6 --> 1001.5: to be addressed. I do believe that it starts with
1001.5 --> 1003.4: that organization and then
1003.4 --> 1005.7: the FSA will also look at those
1006.5 --> 1007.6: recommendations from
1007.6 --> 1009.6: the association and eventually
1009.6 --> 1011.3: that will be mandated as
1012.5 --> 1013.7: what is required
1013.7 --> 1015.7: as not only for a crypto
1015.7 --> 1017.7: company, but
1017.7 --> 1019.9: also eventually for the future of banking
1019.9 --> 1021.6: and eventually for individuals
1022.8 --> 1023.7: who will
1023.7 --> 1024.7: eventually have
1025.6 --> 1027.3: crypto ownership in that sense.
1028.5 --> 1029.8: And it is a good
1030.6 --> 1031.9: start. And I think
1031.9 --> 1033.8: we need to start now.
1033.9 --> 1035.9: And that's a great document. I would love to read tha
t too
1035.9 --> 1037.5: as well. So thank you.
1037.5 --> 1037.9: Thank you.
1044.1 --> 1044.9: Thanks.
1045.2 --> 1046.4: Thanks for this presentation.
1046.9 --> 1049.1: Are you suggesting that
1050.0 --> 1051.5: those documents can
1051.5 --> 1052.9: be shared with
1053.5 --> 1054.7: Begin and that
1055.5 --> 1056.6: maybe Begin can
1057.5 --> 1059.3: think of using part of
1059.3 --> 1060.6: this material to also
1061.5 --> 1062.5: produce a similar

1063.7 --> 1065.0: guidance and
1065.0 --> 1065.5: checklist?
1068.6 --> 1070.7: Yeah, so I'm just thinking
1070.7 --> 1072.8: how to utilize for Begin
1072.8 --> 1074.8: because yesterday
1074.8 --> 1076.9: Begin had many good
1076.9 --> 1078.1: discussions about
1079.0 --> 1081.1: for example MITRE and so on.
1081.2 --> 1082.9: So there are some topics and
1082.9 --> 1085.2: I think this is one topic for
1085.2 --> 1087.3: Begin. And because
1087.3 --> 1088.6: I think
1088.6 --> 1090.8: system vulnerabilities
1090.8 --> 1092.6: are pretty common
1092.6 --> 1093.7: in the world.
1094.4 --> 1096.3: So I think this guideline
1096.3 --> 1098.2: had better help
1098.2 --> 1100.6: for example the US
1100.6 --> 1101.9: and so on.
1102.4 --> 1103.9: But we had better discuss
1104.6 --> 1105.3: how to proceed.
1106.4 --> 1107.4: Yeah, okay.
1108.2 --> 1110.3: I think this is something for us
1110.3 --> 1112.3: also to discuss whether
1112.3 --> 1114.6: there is value to produce
1114.6 --> 1116.1: something around supply chain
1117.5 --> 1118.2: management
1119.4 --> 1120.1: guidance
1121.1 --> 1122.1: specific to
1122.1 --> 1124.1: crypto, blockchain, digital assets
1124.1 --> 1125.0: and so on.
1126.3 --> 1127.7: There are many initiatives
1127.7 --> 1130.0: also on supply chain management,
1130.1 --> 1132.0: security of supply chain outside of
1132.0 --> 1133.8: digital assets. This is not a new topic.
1134.8 --> 1136.2: But considering that
1136.2 --> 1138.3: what you said, not all actors
1138.3 --> 1140.1: in digital
1140.1 --> 1141.9: asset management or at least
1141.9 --> 1143.9: in crypto asset management are necessarily
1143.9 --> 1146.0: mature on cyber security.
1146.3 --> 1148.2: They may not be aware of those.
1148.2 --> 1150.2: So this is something
1150.2 --> 1151.4: we can consider.
1152.0 --> 1154.3: Just conscious that we should also
1154.3 --> 1156.2: avoid not to reinvent the
1156.2 --> 1158.2: wheel and to be sure that we

1158.8 --> 1160.4: stick to specific guidance.
1161.3 --> 1161.8: Otherwise, well,
1162.6 --> 1164.3: I mean, we discussed
1164.3 --> 1165.8: MITRE yesterday.
1166.3 --> 1167.1: There is also
1168.8 --> 1170.1: the CRA
1171.0 --> 1172.2: in EU
1172.2 --> 1174.0: for all what is related to
1175.5 --> 1176.2: SBOM,
1176.2 --> 1178.0: software bill of material.
1178.8 --> 1180.2: There is something which is also
1180.2 --> 1182.0: I think in some of the
1182.0 --> 1184.5: NIST cyber security
1184.5 --> 1186.1: framework documents related
1186.1 --> 1187.8: to the SBOM as well.
1188.3 --> 1190.0: I mean, this is definitely
1190.0 --> 1191.3: not new. However,
1191.8 --> 1193.9: the impact of
1193.9 --> 1196.1: a failure somewhere
1196.1 --> 1197.9: in the supply chain with respect to
1197.9 --> 1200.0: losing access or
1202.0 --> 1202.6: impossibility
1202.6 --> 1204.2: to check transaction and
1204.2 --> 1206.2: really having something
1206.2 --> 1208.3: going wrong that cannot be retrieved is probably
1208.3 --> 1210.0: something which is very specific
1210.0 --> 1212.2: to crypto assets. There are also
1212.2 --> 1214.1: very critical applications that can suffer
1214.1 --> 1216.0: in other domains
1216.0 --> 1218.2: when something is wrong in
1218.2 --> 1220.2: supply chain, but at least we know
1220.2 --> 1222.0: what we are looking at
1222.0 --> 1224.0: in crypto industry.
1227.4 --> 1230.2: I have one question. In one of the
1230.2 --> 1232.1: slides, there was open source
1232.1 --> 1233.6: software and smart contracts
1234.7 --> 1236.3: in the
1236.3 --> 1238.1: list on what can be looked
1238.1 --> 1239.9: at. Have you started something
1239.9 --> 1242.0: in guidance related to open source
1242.0 --> 1244.2: software or this kind of stuff
1244.2 --> 1246.2: or it's focused mostly on managing
1247.2 --> 1248.0: vendors?
1253.1 --> 1255.4: About this topic,
1255.7 --> 1258.2: we are focusing on the pattern
1258.2 --> 1259.9: of the security incident
1259.9 --> 1261.4: rather than the details.

1269.9 --> 1271.3: I think
1271.9 --> 1274.1: to steal
1274.1 --> 1275.7: Bitcoin is
1275.7 --> 1277.1: easy for
1277.9 --> 1278.7: attackers.
1280.4 --> 1281.2: I think
1281.9 --> 1284.0: IoT or some details
1284.0 --> 1285.3: is I think
1285.9 --> 1287.2: the lowest priority
1287.2 --> 1289.2: rather than
1289.2 --> 1290.1: this pattern.
1291.0 --> 1293.1: Because the
1293.1 --> 1295.0: point of the
1295.0 --> 1296.7: attack is for example
1297.2 --> 1299.0: crowd setting and
1299.0 --> 1301.2: some lack
1301.2 --> 1302.4: of the setting.
1304.2 --> 1307.0: I think cryptocurrency companies
1307.0 --> 1308.4: or wallet vendors
1309.2 --> 1310.4: doesn't know this
1311.2 --> 1311.7: knowledge.
1313.2 --> 1315.3: We had better focus on this topic
1315.3 --> 1316.8: rather than this topic.
1319.3 --> 1321.3: This guideline was created
1321.3 --> 1322.7: by this requirement.
1323.5 --> 1325.0: Currently, last Friday,
1325.2 --> 1326.9: we discussed about
1326.9 --> 1328.3: the JFSA.
1329.9 --> 1331.3: Sometimes we
1331.3 --> 1333.3: communicate with JFSA
1333.3 --> 1335.4: how to proceed
1335.4 --> 1336.8: this guideline.
1337.5 --> 1338.3: This is official.
1348.1 --> 1348.7: Lack
1348.7 --> 1349.4: of cloud
1350.8 --> 1351.4: services,
1351.9 --> 1353.4: security controls or
1354.3 --> 1355.7: misconfiguration is definitely
1355.7 --> 1357.7: one of the factors on those attacks.
1357.9 --> 1358.4: But I guess
1361.0 --> 1361.6: some
1361.6 --> 1363.6: issues that we see maybe not
1363.6 --> 1365.7: on those one but on some
1365.7 --> 1367.6: other attacks which happen not
1367.6 --> 1369.8: on exchanges but maybe more
1369.8 --> 1371.0: on the DeFi side.
1372.0 --> 1373.8: This year, we are also related

1373.8 --> 1375.2: to some open source
1377.5 --> 1377.8: vulnerabilities.
1379.6 --> 1381.2: I'm saying that because
1382.4 --> 1383.9: what may happen
1383.9 --> 1385.5: or what already happened
1385.5 --> 1387.8: in some cases is that
1388.8 --> 1389.6: the
1389.6 --> 1391.1: wallet or the
1391.8 --> 1393.8: trading software
1394.3 --> 1395.8: provider in some of the
1395.8 --> 1396.7: exchanges got
1398.0 --> 1399.8: exploited because they
1399.8 --> 1401.7: were using a vulnerable open
1401.7 --> 1402.6: source software as well.
1403.8 --> 1405.6: It's also important, I think, to
1405.6 --> 1408.1: consider the SBOM management.
1408.7 --> 1411.0: I think so because
1411.7 --> 1413.5: the situation is dramatically
1413.5 --> 1415.4: changing. In the past,
1415.7 --> 1417.9: the target was a cryptocurrency company
1417.9 --> 1419.7: but next is a wallet vendor.
1420.4 --> 1421.6: I think in the future,
1422.1 --> 1423.8: open source and other
1423.8 --> 1425.7: patterns will be
1425.7 --> 1426.2: targeted.
1427.7 --> 1429.2: We want to
1430.0 --> 1430.5: protect
1431.7 --> 1433.4: this situation by using
1433.4 --> 1435.1: this guideline. But this guideline
1435.1 --> 1437.0: is one of the guidelines.
1438.3 --> 1439.4: But I think
1439.4 --> 1441.3: it's a good timing
1442.7 --> 1443.5: how to
1443.5 --> 1444.8: utilize in BG.
1448.4 --> 1449.3: If I can
1449.3 --> 1451.4: add to that, if you can go back to
1451.4 --> 1453.2: a few slides before,
1453.4 --> 1455.4: I believe. Yes, this
1455.4 --> 1457.3: one right here. In the case of
1457.3 --> 1459.4: DMM, it was a very unique
1459.4 --> 1460.3: attack.
1461.5 --> 1462.7: With DMM,
1463.2 --> 1465.2: yes, it was a supply chain attack. You're
1465.2 --> 1467.2: correct on that. It just happens
1467.2 --> 1469.2: to be that supply chain was a software
1469.2 --> 1470.9: vendor or developer or system
1470.9 --> 1472.8: integrator. And

1472.8 --> 1474.3: one of the employees
1476.0 --> 1477.3: was underpaid
1477.3 --> 1478.5: and
1479.3 --> 1480.9: basically was given a
1480.9 --> 1483.1: malicious link to click on and hence
1483.1 --> 1484.8: acquiring access to the
1484.8 --> 1485.3: IPC.
1486.8 --> 1487.4: And hence,
1488.8 --> 1489.7: there is a problem there.
1490.5 --> 1492.3: The fact that that employee
1492.3 --> 1494.3: actually had keys to the
1494.3 --> 1496.5: wallets that contained millions of dollars.
1496.6 --> 1498.6: That was just a process risk
1498.6 --> 1500.2: that could have been completely
1500.2 --> 1500.7: avoided.
1503.3 --> 1506.2: And given that he was underpaid and he was
1506.2 --> 1508.2: looking for a job, kind of
1508.2 --> 1509.3: tells you that
1510.5 --> 1512.4: and he had access to
1512.4 --> 1514.5: a few hundred million dollars in that sense
1514.5 --> 1516.4: too. It's worrying.
1516.5 --> 1517.6: It keeps me up at night.
1518.4 --> 1520.5: You have to think, how many of
1520.5 --> 1522.2: these other exchanges
1522.2 --> 1524.4: have that similar problem?
1525.5 --> 1526.5: And I'm
1526.5 --> 1528.4: sure it's pretty prevalent now
1528.4 --> 1530.3: that we saw this actually
1530.3 --> 1532.3: on the top nine
1532.3 --> 1534.2: list of attacks.
1534.5 --> 1535.8: I'm sure there's other exchanges
1536.4 --> 1537.2: that do this.
1538.0 --> 1540.0: Yes, supply chain attack is real.
1541.0 --> 1541.4: But
1542.1 --> 1543.8: supply chain attacks were just
1543.8 --> 1545.7: fundamental attacks. This is not a Web
1545.7 --> 1547.7: 3 problem. This was also a Web 2
1547.7 --> 1548.9: problem as well.
1550.5 --> 1551.8: I used to run a database
1551.8 --> 1553.6: company in my
1553.6 --> 1555.5: previous life in the Web 2 world.
1555.7 --> 1556.7: It was called MySQL.
1557.7 --> 1559.3: And the thing is that
1560.0 --> 1561.3: we were a vendor
1561.3 --> 1563.6: and we had to work with a lot
1563.6 --> 1565.4: of system
1566.0 --> 1567.4: integrators and we had a lot of open source

1567.4 --> 1569.3: contributions and we needed to make sure
1569.3 --> 1571.3: that the push into
1571.3 --> 1573.5: our code base was not malicious
1573.5 --> 1575.3: in nature. What we're seeing
1575.3 --> 1577.4: right now in open source
1577.4 --> 1579.1: software for example is that
1579.1 --> 1581.2: there is malicious code that's being injected
1581.2 --> 1581.7: by
1583.6 --> 1585.4: nation states in that sense
1585.4 --> 1587.1: and being able to infiltrate
1587.1 --> 1589.1: open source code and
1589.1 --> 1591.4: hit security libraries so they can do
1593.4 --> 1593.4: more.
1594.4 --> 1594.8: It's a
1594.8 --> 1596.6: different type of level of supply
1596.6 --> 1598.2: chain where it's at a code level.
1599.4 --> 1600.7: Yes, this
1600.7 --> 1602.5: is correct in regards to
1602.5 --> 1603.6: being able to
1604.3 --> 1606.5: not only know where all your codes
1606.5 --> 1608.7: and all the code dependencies are coming from,
1608.9 --> 1610.7: being able to audit that. That's a lot
1610.7 --> 1611.3: of work.
1612.6 --> 1614.3: Luckily a lot of it's documented.
1615.1 --> 1616.3: Most part of it is
1616.3 --> 1618.2: there's probably some that are not.
1618.8 --> 1620.6: It is a good process and it's something
1620.6 --> 1622.6: to definitely look at in that sense.
1629.1 --> 1629.7: Thank you.
1629.7 --> 1630.3: Daniel, you mentioned
1630.3 --> 1632.7: lack of processes or at least
1632.7 --> 1634.1: lack of
1634.8 --> 1636.6: security maturity
1636.6 --> 1638.5: in the processes for some of the vendors
1638.5 --> 1640.1: in some of those acts.
1640.7 --> 1642.3: I was wondering if there are some
1642.3 --> 1643.7: in the checklist that
1644.4 --> 1646.3: you've shown, if there are some
1646.3 --> 1648.6: controls that are targeting
1648.6 --> 1650.3: the vendors directly. Whether
1650.3 --> 1652.3: basically the controls are only for
1652.3 --> 1654.2: the exchange
1654.2 --> 1656.2: or whether there are some controls
1656.2 --> 1658.3: that need to be checked on the vendor side.
1658.6 --> 1660.2: Because it's one thing to have
1660.2 --> 1662.3: contracts and to say, to remind to the vendor
1662.3 --> 1664.3: well you need to be responsible, liable

1664.3 --> 1666.3: etc. That's another
1666.3 --> 1668.4: thing to know exactly what they consider
1668.4 --> 1670.3: in terms of risk and how
1670.3 --> 1672.0: they mitigate those risks and
1672.9 --> 1674.3: basically which kind of
1674.3 --> 1676.1: controls are in place so that
1676.1 --> 1677.7: the integrators,
1678.1 --> 1680.0: the exchange
1681.7 --> 1682.4: manage
1682.4 --> 1683.4: on the exchange side
1684.0 --> 1685.9: to know basically which
1685.9 --> 1688.0: other mitigation needs to be put in
1688.0 --> 1689.4: place in order to kind of
1690.0 --> 1692.0: strengthen what has
1692.0 --> 1693.9: been taken in account
1693.9 --> 1695.4: or not by the vendor.
1696.3 --> 1697.0: Which is
1699.0 --> 1700.2: typical issue
1700.2 --> 1701.8: when managing vendors
1701.8 --> 1704.0: for your supply chain management
1704.8 --> 1705.4: but
1706.0 --> 1708.1: when you know exactly
1708.1 --> 1708.9: the threats that
1708.9 --> 1711.9: you are facing, this is something
1711.9 --> 1713.5: that you want to, in general,
1713.8 --> 1715.8: to deep dive with vendors.
1718.1 --> 1719.1: Is there anything?
1725.9 --> 1727.1: Anyway, so
1728.8 --> 1730.0: you explained
1730.0 --> 1731.8: the pattern
1731.8 --> 1733.5: is changing in the
1735.1 --> 1736.1: world of vendors
1736.1 --> 1737.6: and this is a bit
1738.1 --> 1739.6: different from the
1740.1 --> 1741.5: Web2 or the current
1742.1 --> 1743.8: legacy systems but
1743.8 --> 1745.5: I think the fundamental
1746.1 --> 1746.4: is
1748.1 --> 1749.7: common because
1749.7 --> 1751.4: so because
1752.1 --> 1753.2: we, so sorry,
1753.8 --> 1755.7: the cryptocurrency company and
1755.7 --> 1757.0: wallet vendors
1758.1 --> 1759.3: have used
1760.1 --> 1761.6: cloud system easily
1762.1 --> 1763.9: and after that
1763.9 --> 1766.0: so probably we don't

1766.0 --> 1767.8: know, we don't need to know
1767.8 --> 1768.6: the details
1768.6 --> 1771.2: to use the cloud.
1771.6 --> 1773.4: So this is one lack of the
1773.4 --> 1775.6: point. So I think so
1775.6 --> 1777.7: important thing is how to educate
1777.7 --> 1779.1: how to teach
1779.1 --> 1781.1: the members
1781.1 --> 1783.5: about the security in terms of the
1783.5 --> 1785.7: setting and so on. So I think
1785.7 --> 1786.8: important thing is
1787.7 --> 1789.5: my first priority
1789.5 --> 1792.0: is how to input
1792.0 --> 1793.9: this information
1793.9 --> 1795.7: into the members.
1797.0 --> 1797.9: This is first
1797.9 --> 1799.3: important thing.
1805.0 --> 1806.1: I agree.
1806.8 --> 1808.2: It's always an escalation
1808.2 --> 1810.1: of attack vectors. Right
1810.1 --> 1812.0: now they are targeting wallets, it's obvious.
1812.5 --> 1814.2: I think a good example
1814.2 --> 1816.0: of this is that when the hackers
1816.0 --> 1818.4: exploited the Web2
1818.4 --> 1820.0: infrastructure for Trezor, for example,
1820.0 --> 1821.2: and drained
1821.9 --> 1824.1: the contact email lists of
1824.1 --> 1825.4: all their users.
1826.3 --> 1828.0: And now I get at least
1828.0 --> 1830.3: about five emails from Trezor
1830.3 --> 1832.0: saying that I need to
1832.0 --> 1832.9: upgrade my wallet.
1833.9 --> 1836.1: And you don't
1836.1 --> 1838.0: know which links to click
1838.0 --> 1839.9: as a user. And if it was my
1839.9 --> 1841.9: you know, if it was my father
1841.9 --> 1844.1: who's 84 years old, he would not know
1844.1 --> 1845.1: he would click it.
1846.2 --> 1848.4: And if anything, it's also
1848.4 --> 1849.2: I mean,
1850.6 --> 1852.5: Trezor doesn't put it on
1852.5 --> 1854.1: their top page saying,
1854.3 --> 1856.2: look, you only accept emails
1856.2 --> 1857.8: from this, you know, things.
1857.9 --> 1860.4: Even the wallet vendors need
1860.4 --> 1862.3: to make that effort to notify
1863.5 --> 1864.1: announcements

1864.1 --> 1866.2: or anything, please check our
1866.2 --> 1867.9: website for the official announcements.
1868.1 --> 1870.3: We did that when we were doing as a database vendor.
1870.9 --> 1872.4: Right. And so as a wallet
1872.4 --> 1874.1: company, they have that duty
1874.1 --> 1876.4: to know that only accept or read
1878.2 --> 1878.7: updates
1878.7 --> 1880.0: from this website as
1880.0 --> 1882.4: a certified source of information.
1882.9 --> 1884.3: And the same thing, you see it on crypto
1884.3 --> 1885.6: Twitter at the same time.
1886.0 --> 1888.1: People were saying airdrops or whatever
1888.1 --> 1890.3: because they're always looking for any attack
1890.3 --> 1892.3: vectors to get access to your
1892.3 --> 1894.3: wallet. And it's
1894.3 --> 1896.3: a wallet attack now. And so
1896.3 --> 1898.1: eventually it's going to be
1898.1 --> 1900.1: social engineering attacks. And
1900.1 --> 1901.8: that I get on, I get at least
1902.4 --> 1904.2: two calls a month from Binance
1904.2 --> 1906.1: saying that, you know, that
1906.1 --> 1907.8: they've halted my
1907.8 --> 1910.1: Binance account. And I'm like, that's strange,
1910.2 --> 1911.3: I don't have a Binance account.
1911.9 --> 1913.2: But the thing is,
1914.9 --> 1916.1: it's getting down to
1916.1 --> 1918.1: that level and their attacks are getting
1918.1 --> 1920.1: more sophisticated and
1920.7 --> 1922.1: people are doing this more
1922.1 --> 1924.5: and we do need to have that level of education
1924.5 --> 1925.2: in that sense.
1931.5 --> 1932.3: Should we look
1932.3 --> 1933.9: at the checklist that you
1933.9 --> 1934.9: briefly
1937.1 --> 1938.4: shared in order to see
1938.4 --> 1940.3: where, or just to have an understanding of
1940.3 --> 1942.2: the level of controls
1942.2 --> 1943.8: that are defined on the checklist?
1945.6 --> 1946.4: If you want to
1946.4 --> 1947.1: share it again.
1949.5 --> 1949.9: No,
1950.1 --> 1952.2: but so, yes,
1953.2 --> 1954.3: so that's it for my
1954.3 --> 1956.0: presentation. And
1956.0 --> 1958.2: I, sorry, I would like to
1958.2 --> 1960.0: know your
1960.0 --> 1961.8: comment about this topic,

1962.0 --> 1963.6: how to proceed it or not.
1964.3 --> 1966.2: Because, so this is
1966.2 --> 1968.2: just a first step.
1969.9 --> 1971.4: Yeah, that's why
1972.0 --> 1974.1: if you can come back to one of
1974.1 --> 1975.3: the documents that you shared,
1976.2 --> 1977.6: particularly I think the checklist,
1978.1 --> 1979.9: maybe we can have, I mean, if
1979.9 --> 1982.1: it's possible, we can have a look just to understand
1982.1 --> 1984.0: better the level of details and
1984.0 --> 1984.6: how we
1985.6 --> 1988.1: can help, whether we can reuse
1988.1 --> 1988.8: part of it.
1989.8 --> 1992.1: Okay, I'll share this
1992.1 --> 1992.8: checklist.
1996.2 --> 1997.9: There is clearly
1997.9 --> 1999.7: a need to educate
1999.7 --> 2001.4: further, I mean,
2001.6 --> 2004.2: and it's true for other
2004.2 --> 2005.1: industries as well.
2006.6 --> 2007.8: The more,
2008.3 --> 2009.4: the easier
2010.1 --> 2011.4: the tools for
2012.5 --> 2013.4: deploying,
2014.2 --> 2015.7: well, for developing first
2016.8 --> 2017.7: by coding
2017.7 --> 2019.9: for deploying, for defining
2019.9 --> 2021.6: infrastructure and
2021.6 --> 2024.0: the more we need them to educate
2024.0 --> 2026.4: that, well, transversal
2026.4 --> 2027.8: security configuration,
2028.1 --> 2030.2: security controls, all those things, because
2030.2 --> 2031.8: if they are not by default, of course,
2032.1 --> 2033.7: they are not made. But yeah.
2039.8 --> 2041.8: Yes, yes.
2047.3 --> 2048.9: Are you there?
2049.4 --> 2051.0: Yes, yes. Can you hear me?
2051.4 --> 2051.5: Yes.
2052.3 --> 2054.9: I think it's
2054.9 --> 2057.0: better to share this checklist.
2057.3 --> 2057.8: Is it okay?
2059.2 --> 2061.0: I think it's okay.
2061.2 --> 2062.3: Yeah, but we have to check
2062.3 --> 2063.1: internally.
2064.4 --> 2066.8: Maybe it's better
2066.8 --> 2068.8: to proceed this kind of
2068.8 --> 2069.6: document sharing.

2078.9 --> 2079.8: Yeah.
2080.1 --> 2080.8: In the,
2082.1 --> 2083.9: in this list,
2086.1 --> 2087.0: while
2087.0 --> 2088.7: you discussed establishing
2089.7 --> 2091.9: the list and defining the content
2091.9 --> 2093.5: with your members in
2093.5 --> 2095.8: GP, CryptoISAC,
2096.3 --> 2097.2: is there anything
2097.2 --> 2099.4: that you can share on
2099.4 --> 2102.0: some specific items
2102.0 --> 2103.5: that were really considered
2103.5 --> 2105.2: as unclear
2106.1 --> 2108.0: from the members or
2108.0 --> 2110.3: some specific items that are
2110.3 --> 2112.2: considered as very specific to
2112.2 --> 2113.2: cryptoassets?
2114.1 --> 2116.4: I mean, just to avoid to look
2116.4 --> 2118.2: at all of them one by one,
2118.4 --> 2120.3: which can take quite some time.
2123.5 --> 2125.4: Yeah, yeah, yeah. I think that these
2125.4 --> 2127.2: kind of documents are based on the FISC.
2127.3 --> 2129.0: So I think that it's a true advice.
2129.6 --> 2131.2: So maybe there's, I think there's
2131.2 --> 2132.4: some technical
2133.2 --> 2133.9: checklists
2133.9 --> 2136.1: will be important.
2136.7 --> 2138.3: I think that since you
2138.3 --> 2140.3: discussed DeFi or
2140.3 --> 2142.0: Web3, so
2142.0 --> 2144.7: yeah, I think that this is based on
2144.7 --> 2146.3: the really traditional ones.
2146.7 --> 2148.7: So yeah, it's better to
2148.7 --> 2150.8: cover. I think the main feature
2150.8 --> 2152.7: of this checklist is
2152.7 --> 2154.4: the crown setting.
2156.6 --> 2158.8: because, so as I explained
2158.8 --> 2160.5: to you, so some,
2160.5 --> 2160.9: sorry.
2172.6 --> 2174.0: Sorry.
2180.5 --> 2182.6: So sometimes
2182.6 --> 2184.6: cryptocurrency companies and
2184.6 --> 2186.3: web vendors had better
2186.3 --> 2188.5: know the setting, how
2188.5 --> 2189.7: to set the crowd
2190.5 --> 2192.5: because the
2192.5 --> 2194.5: first attempt from

2194.5 --> 2196.2: the attackers is
2196.2 --> 2198.4: the phishing.
2199.3 --> 2200.1: But finally,
2200.7 --> 2201.9: they would like to
2202.5 --> 2204.3: steal the access
2204.3 --> 2206.5: key or access
2206.5 --> 2207.9: key of the crowd.
2209.1 --> 2210.6: So, for
2210.6 --> 2212.6: example, one sample
2212.6 --> 2214.2: is how to separate
2214.2 --> 2216.2: environment between the
2216.2 --> 2217.7: test environment
2217.7 --> 2219.2: and production environment.
2220.5 --> 2221.6: So this is
2221.6 --> 2223.3: the Web2,
2223.6 --> 2225.7: so for Web2 company
2225.7 --> 2227.8: it's common.
2228.2 --> 2229.9: On the other hand, cryptocurrency
2229.9 --> 2231.8: company sometimes doesn't know
2231.8 --> 2234.0: this, including world vendors.
2235.1 --> 2236.0: So, but
2236.0 --> 2237.9: anyway, so this is for
2237.9 --> 2239.6: the world vendors
2240.2 --> 2242.1: how to understand this.
2243.4 --> 2243.6: But
2243.6 --> 2245.5: the today's,
2245.5 --> 2247.6: I think so the today's topic is
2247.6 --> 2249.4: how to
2249.4 --> 2251.8: share this information
2251.8 --> 2252.5: to
2253.5 --> 2256.0: begin or external
2256.0 --> 2256.9: members
2257.6 --> 2259.3: or in terms of
2259.3 --> 2262.4: education or so on.
2264.0 --> 2265.7: So I would like to
2265.7 --> 2266.9: know your
2267.6 --> 2268.1: opinion.
2270.3 --> 2271.5: And in Japan, so
2271.5 --> 2272.2: JPEG
2272.2 --> 2274.0: will proceed
2274.0 --> 2277.0: to update this
2277.5 --> 2279.2: document with company
2279.2 --> 2279.8: members.
2291.5 --> 2293.1: Sorry, this checklist
2293.1 --> 2294.8: is really detailed, so
2294.8 --> 2296.9: we had better, so I
2296.9 --> 2298.3: don't want to

2298.3 --> 2299.6: explain
2300.3 --> 2302.4: this each
2302.4 --> 2302.8: category.
2316.3 --> 2318.6: I think in principle,
2319.4 --> 2320.2: I think from
2320.2 --> 2322.1: a beginning perspective,
2322.4 --> 2323.0: it's, I mean,
2324.0 --> 2326.0: any educational or
2326.0 --> 2327.8: informative material
2327.8 --> 2329.9: can be useful, but the question is
2329.9 --> 2332.0: whether we produce something that is really
2332.0 --> 2334.0: adding value compared to what
2334.0 --> 2334.9: exists already.
2336.3 --> 2337.7: So I will really
2337.7 --> 2340.0: begin to understand
2340.8 --> 2342.0: how we can
2342.0 --> 2342.8: emphasize
2344.8 --> 2346.2: either based
2346.2 --> 2347.9: on the attack
2347.9 --> 2349.9: path, the attack vectors that have been exploited
2349.9 --> 2351.7: recently, what was missing
2351.7 --> 2354.0: and referring to some
2354.0 --> 2356.0: documents and could be
2356.7 --> 2358.0: your document, can
2358.0 --> 2360.1: be some others as well, can be
2360.1 --> 2362.1: a begin document at the end
2362.1 --> 2363.9: just to say, well,
2364.1 --> 2366.0: you saw, you noticed on those
2366.0 --> 2368.0: attacks, this has been followed.
2370.3 --> 2372.1: Or as an additional,
2372.6 --> 2373.6: as another
2373.6 --> 2376.1: kind of contribution that begin can have,
2376.3 --> 2376.7: I guess,
2377.8 --> 2380.0: could be to really emphasize
2380.0 --> 2381.9: what is specific to cryptoassets.
2382.6 --> 2383.8: And that is not
2383.8 --> 2385.4: well addressed by some other
2387.5 --> 2388.0: frameworks,
2388.1 --> 2388.4: et cetera.
2391.7 --> 2393.0: This way, like this,
2394.0 --> 2395.9: it's hard to tell whether the document by
2395.9 --> 2397.8: itself directly can be leveraged.
2398.2 --> 2400.0: I mean, we need a bit more
2400.0 --> 2401.5: insights, I guess.
2403.7 --> 2404.2: Great.
2405.8 --> 2407.9: I know that my question is
2407.9 --> 2410.0: going to be more based on, I know I was a latecomer

2410.0 --> 2411.9: to this discussion because I was in the other
2411.9 --> 2412.2: room.
2413.4 --> 2415.9: Some of it's going to be me asking for clarity
2415.9 --> 2417.8: to try to help stoke
2417.8 --> 2418.4: some thinking.
2419.6 --> 2421.5: The certification or evaluation
2421.5 --> 2422.2: regime,
2424.2 --> 2424.9: is it
2424.9 --> 2427.9: right that the conversation is more
2427.9 --> 2429.6: around that we want to map where
2429.6 --> 2431.1: existing certification
2431.9 --> 2433.8: regimes sort of exist so that we
2433.8 --> 2434.5: can point to it?
2435.8 --> 2437.4: Is this a consideration of
2437.4 --> 2439.3: whether another one needs to be
2439.3 --> 2441.5: stood up and whether begin wants to stand
2441.5 --> 2443.5: one up, I guess? Or I
2443.5 --> 2445.6: can go backwards. I can start with an easier question.
2445.8 --> 2446.0: All right.
2448.5 --> 2449.7: I agree.
2451.0 --> 2453.5: If the context of all of the controls that we're
2453.5 --> 2454.3: talking about here,
2455.3 --> 2457.6: is it right to assume that we're not just
2457.6 --> 2459.4: talking about the supply chain related
2459.4 --> 2460.7: controls and issues?
2461.1 --> 2463.5: That one's important because just
2463.5 --> 2465.5: like we see in traditional
2465.5 --> 2467.5: finance and many other sectors, supply chain
2467.5 --> 2468.9: ends up being at the heart of most cyber
2469.5 --> 2471.4: compromise. Going after those
2471.4 --> 2473.3: managed service providers is just super
2473.3 --> 2473.8: attractive
2475.7 --> 2477.3: to elicit actors.
2478.3 --> 2479.5: It sounds like
2479.5 --> 2481.3: that yes, this is us thinking
2481.3 --> 2483.4: about the broader conversation that we've been
2483.4 --> 2485.1: having in the other working groups too about
2485.1 --> 2487.0: looking at the attack vector,
2487.5 --> 2489.3: looking at the vulnerability specifically
2489.3 --> 2491.4: that's being compromised, mapping
2491.4 --> 2493.4: that to what the critical controls
2493.4 --> 2495.0: are in each of those instances.
2495.7 --> 2497.6: In a lot of those instances, those standards
2497.6 --> 2499.5: already exist because it's traditional
2499.5 --> 2501.5: standards. In other
2501.5 --> 2503.4: cases, it's exquisite bespoke
2503.4 --> 2505.5: crypto related ones, some which

2505.5 --> 2507.6: already exist from organizations like
2507.6 --> 2509.5: CCSS, and some of it
2509.5 --> 2511.4: points to a big giant gap of
2511.4 --> 2513.1: where standards don't yet exist.
2513.7 --> 2515.6: I do feel that that kind
2515.6 --> 2517.6: of mapping, so I hope
2517.6 --> 2519.5: that this intervention is relevant
2519.5 --> 2521.3: to the conversation. I am sorry if I'm at
2521.3 --> 2523.3: an oblique
2523.3 --> 2525.0: angle to it, but
2525.0 --> 2527.0: truly continuing
2527.0 --> 2528.6: to take that
2530.1 --> 2531.7: attack focused
2533.7 --> 2535.1: mentality of understanding
2535.1 --> 2537.3: the threat, yes, but then
2537.3 --> 2539.1: where that needs to feed into
2539.1 --> 2541.7: the information that's useful to developers
2541.7 --> 2543.7: and engineers and regulators
2543.7 --> 2545.4: is, so what would have defended
2545.4 --> 2546.3: against that?
2547.1 --> 2548.1: Us doing
2548.1 --> 2549.9: a mapping
2549.9 --> 2552.2: based on those vectors of compromise
2552.2 --> 2554.2: to what the vulnerabilities
2554.2 --> 2556.2: are, mapping that to
2556.2 --> 2558.5: the specific controls, just like
2558.5 --> 2559.4: we get
2560.1 --> 2562.6: similar to what NIST did in their ransomware
2562.6 --> 2564.3: threat profile. This would
2564.3 --> 2566.3: be where they
2566.3 --> 2568.1: basically did a mapping of
2568.9 --> 2570.6: all the main points
2570.6 --> 2572.4: of compromise that most ransomware attacks
2572.4 --> 2574.5: come into, and then they mapped
2574.5 --> 2576.5: it to specific controls
2576.5 --> 2578.7: that would have helped defend against it.
2579.1 --> 2580.7: I think that kind of mapping,
2580.9 --> 2582.8: I've never seen that exist
2582.8 --> 2585.0: holistically. There's
2585.0 --> 2586.1: very specific, like
2586.1 --> 2588.9: small parts that are pointed to,
2589.3 --> 2590.3: but something holistic
2590.3 --> 2592.7: that looks at each of those compromises,
2592.8 --> 2594.9: we can prioritize ones that focus on third
2594.9 --> 2596.5: party risk management and
2596.5 --> 2598.8: key compromise, let's be real, that's
2598.8 --> 2600.4: at the heart of most of these breaches,

2601.1 --> 2602.4: so I'd start there
2602.4 --> 2605.1: and then literally just map
2605.1 --> 2607.1: to existing frameworks,
2607.5 --> 2608.6: existing controls.
2609.8 --> 2611.1: Once we know what
2611.1 --> 2613.1: the controls are, that's where then we can
2613.1 --> 2615.0: do a more comprehensive mapping
2615.0 --> 2617.1: of all the different evaluation regimes
2617.1 --> 2618.7: that exist against those.
2620.1 --> 2621.0: At least to
2621.0 --> 2623.0: me, in my head, that's sort of the flow
2623.0 --> 2624.9: that has to come as us doing that mapping
2624.9 --> 2627.1: to what the vulnerabilities
2627.1 --> 2628.9: and controls are
2628.9 --> 2630.8: based on the attack vectors.
2631.5 --> 2633.0: We can use ADAPT as
2633.0 --> 2635.0: that framework. We don't have to start with ADAPT.
2635.0 --> 2636.4: We can just pick our own, but
2637.3 --> 2639.3: I do feel that that would be valuable.
2639.8 --> 2640.9: I don't think that the industry
2640.9 --> 2643.0: has a, like, here's a list of
2643.0 --> 2645.1: all the different kinds of controls, and then as you
2645.7 --> 2646.7: do your own
2646.7 --> 2647.9: risk evaluation
2648.9 --> 2650.9: inside of your compliance programs to
2650.9 --> 2652.8: then go justify to JFSA
2652.8 --> 2654.4: or the SEC or whomever,
2655.8 --> 2656.6: to be able
2656.6 --> 2658.9: to go to to look authoritatively,
2658.9 --> 2660.9: here's all the references that
2660.9 --> 2662.9: I can use because standards
2662.9 --> 2664.8: already exist, and then
2664.8 --> 2666.8: also that will highlight exactly
2666.8 --> 2667.7: where the gaps are.
2669.2 --> 2670.9: And if you look at those gaps
2670.9 --> 2672.8: informed by the threat picture, that
2672.8 --> 2674.9: will help organizations like BEGIN and
2674.9 --> 2676.8: regulators prioritize which standards
2676.8 --> 2678.0: we need to be creating first.
2678.9 --> 2680.7: Anyway, that's my thought on the
2680.7 --> 2681.5: process flow.
2684.1 --> 2684.8: Thank you.
2685.2 --> 2686.9: We're sitting here grinning at each other because
2688.0 --> 2688.5: we...
2690.2 --> 2690.9: No, no.
2691.2 --> 2692.3: No, no, no.
2692.7 --> 2694.6: Because we did have that thing of,

2694.8 --> 2696.6: you know, should we be doing this in the realization that
2698.0 --> 2698.6: as you
2698.6 --> 2700.6: intuited, like, 98%
2700.6 --> 2701.6: of it's already there.
2702.4 --> 2704.6: And so it's actually counterproductive
2705.2 --> 2706.5: to try to do it again,
2706.5 --> 2708.6: but it is a value to the community
2709.7 --> 2710.9: to have that
2711.7 --> 2712.7: list, the map,
2712.9 --> 2714.6: you know, the list of things to...
2714.6 --> 2716.5: And yeah, we didn't quite think of it, but yeah,
2716.5 --> 2718.4: I'm sure there's some big, huge gap that
2718.4 --> 2720.5: we could fill, but we
2720.5 --> 2722.2: didn't actually kind of run into it.
2722.6 --> 2724.4: That's also not unuseful to highlight
2724.4 --> 2726.3: to the industry. Like, from a regular...
2726.3 --> 2728.3: Yeah, sorry. That's a great point. I loved
2728.3 --> 2730.5: Eric bringing that up, that, like, from a
2730.5 --> 2731.9: regulatory perspective,
2732.3 --> 2734.9: for me, like, why I...
2734.9 --> 2736.5: Why we had had standards
2736.5 --> 2738.3: work prioritized in the competitiveness
2738.3 --> 2740.5: framework and the EO for digital
2740.5 --> 2742.1: assets under President Biden
2742.1 --> 2744.4: was because, like, it would have
2744.4 --> 2746.5: been a really great tool if we had
2746.5 --> 2748.1: had something output
2749.0 --> 2749.8: to us,
2751.1 --> 2751.5: whether
2752.1 --> 2754.5: from industry or from agencies, that basically
2754.5 --> 2756.5: we could say, oh, look, all of this is actually
2756.5 --> 2758.6: just an implementation of long-existing standards
2758.6 --> 2760.7: problems. So this is about implementation
2760.7 --> 2762.5: and enforcement, not about a policy
2762.5 --> 2764.1: problem or standards, because
2764.1 --> 2766.3: industry comes in and claims and points
2766.3 --> 2768.2: to standards. Like, we see this all the time in
2768.2 --> 2770.6: tons of issues, including, like...
2770.6 --> 2772.5: And some things are fair and some things are not,
2772.5 --> 2774.5: but, like, being able to help, like,
2775.6 --> 2776.5: pierce through the
2776.5 --> 2778.3: mist of, like, of...
2778.3 --> 2780.1: And the fog of what's
2780.1 --> 2782.5: truly the issue, is this
2782.5 --> 2784.5: because we don't know how to do it
2784.5 --> 2786.4: and there isn't a policy around it

2786.4 --> 2788.4: and maybe our policy
2788.4 --> 2790.5: isn't aligned to the practical reality
2790.5 --> 2791.4: of what needs to happen,
2792.5 --> 2794.3: or is it, like...
2794.3 --> 2795.9: Or is this actually an implementation
2796.5 --> 2798.6: problem? So this is more industry and then
2798.6 --> 2800.5: enforcement, as
2800.5 --> 2802.8: carrots and sticks
2802.8 --> 2804.8: for incentives. So I think that
2804.8 --> 2806.7: that kind of mapping would be really valuable
2806.7 --> 2808.7: and probably not that hard,
2809.1 --> 2810.8: given all the great work that's
2810.8 --> 2811.9: already been done by
2813.0 --> 2814.8: us and MITRE and
2814.8 --> 2815.5: JFSA
2818.1 --> 2818.7: and
2818.7 --> 2820.6: organizations like CCSA, since they're here.
2822.8 --> 2824.7: Sorry, I didn't mean to keep
2824.7 --> 2825.3: talking over you.
2826.2 --> 2828.6: I'm pretty much supportive of what
2828.6 --> 2830.2: Julien and Carol have
2830.2 --> 2832.3: talked about, and
2832.3 --> 2834.7: would you mind putting
2834.7 --> 2836.5: the slides that
2836.5 --> 2838.4: shows the good practices,
2838.7 --> 2840.4: guidelines, purpose, and positioning?
2842.7 --> 2844.2: I just wanted to clarify
2844.2 --> 2846.7: how the guidelines, the role of the
2846.7 --> 2848.7: guidelines, and
2848.7 --> 2850.6: it was page three,
2850.8 --> 2851.4: I believe.
2861.0 --> 2862.4: Over here.
2865.8 --> 2866.7: Yes, this.
2868.7 --> 2869.2: As
2869.2 --> 2870.3: just an experience,
2870.6 --> 2872.6: actually, I have
2872.6 --> 2874.2: experience with the
2874.2 --> 2876.7: second to the FIAC in the
2876.7 --> 2878.7: past, and the
2878.7 --> 2880.8: role of the FIAC guidelines
2880.8 --> 2882.9: is showing the perspectives.
2883.9 --> 2884.6: Did you see this?
2884.7 --> 2886.5: Did you see this? That kind of
2886.5 --> 2887.2: perspective
2890.5 --> 2892.0: to be checked,
2892.4 --> 2894.0: not only by the
2894.0 --> 2896.6: crypto industry, but also

2896.6 --> 2898.3: the traditional banks
2898.3 --> 2900.4: and insurance companies, any type
2900.4 --> 2901.9: of financial service companies.
2903.4 --> 2904.4: And it's not
2904.4 --> 2906.4: a certification program, so
2906.4 --> 2908.2: it doesn't assure what
2908.2 --> 2909.1: level of the
2910.0 --> 2912.5: kind of practices
2912.5 --> 2913.8: did you do,
2913.8 --> 2915.8: but just kind of perspectives.
2917.2 --> 2917.6: Hence,
2919.3 --> 2921.8: the things, the evolving
2921.8 --> 2923.8: part of the information
2923.8 --> 2925.9: sharing is, as
2925.9 --> 2927.6: you highlighted
2927.6 --> 2929.6: on the right-hand side part.
2930.4 --> 2931.9: So perhaps we
2931.9 --> 2933.7: may want to share
2933.7 --> 2935.8: the information on the
2935.8 --> 2936.8: evolving part,
2938.1 --> 2939.9: not only what's experienced
2939.9 --> 2942.0: in Japan, but also what
2942.0 --> 2943.0: is experienced in the world.
2944.0 --> 2944.9: Carol said that
2946.0 --> 2948.0: Eric said
2948.0 --> 2949.2: that it may
2949.2 --> 2952.0: 98% also prevailing,
2952.7 --> 2954.0: but it hasn't
2954.0 --> 2956.0: compiled to
2956.0 --> 2957.5: be seen in the easy
2957.5 --> 2959.7: to see part.
2960.3 --> 2960.9: So perhaps
2960.9 --> 2963.4: we may collaborate
2964.0 --> 2965.4: each other to what
2966.0 --> 2966.8: JPCrypt, Isaac
2968.0 --> 2969.9: kind of accumulated, and
2969.9 --> 2971.8: some other parts of
2971.8 --> 2973.9: the world could share
2973.9 --> 2975.6: if it is a public
2975.6 --> 2977.7: knowledge, but just
2977.7 --> 2979.8: as to be seen easily
2979.8 --> 2982.0: by
2982.0 --> 2983.4: the members or by
2983.9 --> 2985.5: any community.
2986.6 --> 2986.7: So
2988.2 --> 2989.3: again,
2990.0 --> 2990.8: with the

2991.9 --> 2993.2: basic pillars
2993.9 --> 2995.9: on the right-hand side
2995.9 --> 2997.9: plus the evolving
2997.9 --> 3000.1: part, which can
3001.3 --> 3002.2: benefit
3002.2 --> 3004.1: not only the crypto exchanges,
3004.3 --> 3004.8: but also
3006.2 --> 3008.2: those in the supply chain
3008.2 --> 3009.9: who might be
3009.9 --> 3011.0: especially
3011.9 --> 3013.8: need to be registered with
3013.8 --> 3015.9: the JFSA in the coming
3015.9 --> 3016.6: years.
3018.2 --> 3019.0: Again,
3019.9 --> 3021.3: it will be helpful
3021.9 --> 3023.7: to, let's say, how
3023.7 --> 3025.9: the level of the
3028.5 --> 3029.2: means
3029.9 --> 3031.3: to protect the customers.
3032.3 --> 3033.7: Certainly, it's kind of
3033.7 --> 3035.6: evolving. It doesn't say
3036.6 --> 3037.5: there's no
3037.5 --> 3039.7: fixed level of the assurance
3041.2 --> 3041.9: to
3041.9 --> 3043.5: satisfy that
3043.5 --> 3044.0: protection.
3051.9 --> 3053.9: To add to that, I think you guys
3053.9 --> 3055.7: all have great points, but
3055.7 --> 3057.7: I mean, this is the stuff that keeps
3057.7 --> 3059.9: the CSO awake at night,
3060.8 --> 3061.8: and whether
3061.8 --> 3063.7: if it's certifications or
3063.7 --> 3065.7: assurances and providing that.
3066.3 --> 3067.7: I mean, it's always
3067.7 --> 3069.7: an ever-chasing rabbit
3070.5 --> 3071.8: and the carrot
3071.8 --> 3073.1: and the stick action.
3074.1 --> 3075.0: I think,
3075.5 --> 3077.6: but yes, they
3077.6 --> 3079.7: need to be certified or use reference-certified
3080.4 --> 3081.9: products and stuff like that,
3082.4 --> 3083.1: but
3083.9 --> 3085.2: what's it to them
3085.2 --> 3086.8: to immediately do it, too?
3087.2 --> 3089.4: I mean, of course, the fact that the CSO
3089.4 --> 3091.4: could sleep at night. I mean, other CXOs
3091.4 --> 3093.0: just want to go, go, go, go

3093.0 --> 3094.9: and release and just
3095.6 --> 3097.1: get something out
3097.1 --> 3098.6: there versus
3099.4 --> 3101.2: break things and fix it
3101.2 --> 3102.6: and move on, in that sense.
3103.7 --> 3104.9: Fortunately, in crypto,
3105.1 --> 3106.7: if you break it, you lose millions.
3108.1 --> 3109.3: In this sense,
3110.7 --> 3111.7: of course,
3111.8 --> 3113.4: the framework is still being designed,
3113.6 --> 3115.3: and I think a checklist is really needed.
3116.4 --> 3116.9: I think
3117.7 --> 3118.2: the
3122.3 --> 3122.8: JVCA,
3123.0 --> 3123.3: the
3123.3 --> 3124.1: association,
3125.7 --> 3127.3: they're also in talks about
3127.3 --> 3129.5: kind of putting a layer of insurance.
3129.7 --> 3131.4: To qualify insurance, I think you
3131.4 --> 3133.4: would need certain certifications, for example,
3133.4 --> 3135.0: to be able to know that
3135.0 --> 3137.1: the system is designed in this sense,
3137.1 --> 3139.1: so it can be underwrited and insured.
3140.2 --> 3141.4: There needs to be
3141.4 --> 3142.1: some form of
3144.0 --> 3145.6: motivator, in that sense, to be
3145.6 --> 3147.1: in compliance or
3147.6 --> 3148.0: actually
3149.3 --> 3150.9: using certain specs
3150.9 --> 3153.2: or certified components,
3153.3 --> 3155.4: in that sense. I think insurance
3155.4 --> 3157.3: or something of that nature, a financial
3158.1 --> 3159.2: motivator, in that sense,
3159.2 --> 3161.5: aside from losing a lot of millions of dollars in cap
ital
3161.5 --> 3162.7: if you get hacked,
3164.7 --> 3165.1: I think
3165.1 --> 3167.0: also being able to
3167.0 --> 3169.0: do risk management better,
3169.2 --> 3171.4: in that sense, and having a financial
3171.4 --> 3173.1: incentive around that and
3173.1 --> 3175.4: creating that would probably be something.
3175.7 --> 3177.6: I see in the future,
3177.7 --> 3179.2: probably not today, but
3179.2 --> 3181.6: maybe tomorrow or in a few years
3181.6 --> 3183.6: from now, that insurance companies
3183.6 --> 3185.5: will probably underwrite cryptocurrency

3185.5 --> 3187.5: companies or crypto companies, for that
3187.5 --> 3189.7: matter. We're seeing kind of headways
3189.7 --> 3191.7: in that in Hong Kong, for example,
3192.7 --> 3193.6: and probably
3193.6 --> 3195.4: in the United States. Maybe you can answer to that.
3196.4 --> 3196.6: No.
3198.9 --> 3199.7: I'm not
3199.7 --> 3201.9: sure I'll credit too much progress
3201.9 --> 3203.6: in the... That's not totally
3203.6 --> 3205.6: fair of me. It's a little fair of me, but not totally.
3206.8 --> 3207.7: I was actually
3207.7 --> 3209.2: going to reference the Hong Kong example
3209.2 --> 3211.6: that just at the roundtable that we had on
3211.6 --> 3212.9: Friday that you were talking about,
3214.1 --> 3214.5: Ryan
3216.0 --> 3217.2: had mentioned that
3219.0 --> 3219.6: part of the
3219.6 --> 3221.4: way that... Hong Kong has some very
3221.4 --> 3223.0: prescriptive measures in their
3223.0 --> 3225.3: regulatory obligations, and I'm
3225.3 --> 3227.3: really curious to dig into
3227.3 --> 3229.3: that because I mentioned the
3229.3 --> 3231.2: challenge that as regulators we had
3232.2 --> 3233.1: on... Frankly,
3233.3 --> 3235.4: we would get criticized if the requirements
3235.4 --> 3237.7: were rules-based or if they were risk-based.
3237.7 --> 3239.5: If they were rules-based, they were too prescriptive,
3239.6 --> 3241.5: they weren't future-proof, they didn't
3241.5 --> 3243.3: evolve enough, they didn't allow for
3243.3 --> 3244.7: risk-based implementations,
3245.2 --> 3247.4: and if they were risk-based, then they weren't clear
enough
3247.4 --> 3249.1: and institutions didn't know what to do.
3249.1 --> 3250.5: Understanding
3251.1 --> 3252.7: that there's that challenge,
3253.8 --> 3255.4: it's really neat to see
3255.4 --> 3257.5: industry respond well to
3257.5 --> 3259.1: the Hong Kong approach of having
3259.8 --> 3261.0: very specific,
3261.4 --> 3263.5: highly critical, high-impact
3263.5 --> 3265.4: prescriptive measures, and then
3265.4 --> 3267.4: having a requirement for
3267.4 --> 3268.7: crypto insurance.
3269.6 --> 3271.5: Turning to the natural market
3271.5 --> 3272.9: lever and incentive that
3272.9 --> 3274.8: allowing the industry to decide
3274.8 --> 3277.4: who's going to insure these guys and those

3277.4 --> 3279.4: guys are interested in making sure that their securit
y
3279.4 --> 3281.0: is good because I know that this is the top
3281.0 --> 3282.7: threat of them losing
3283.6 --> 3285.3: a lot of money there
3285.3 --> 3287.3: besides maybe underwriting value of
3287.3 --> 3289.3: assets, depending on the use
3289.3 --> 3289.5: case.
3292.1 --> 3293.2: I agree.
3293.6 --> 3295.2: I think that that kind of
3295.2 --> 3297.3: category, at least
3297.3 --> 3299.3: on thinking about whether or not
3299.3 --> 3301.1: it is valuable to do this mapping
3301.1 --> 3303.6: of controls and then two different certification
3303.6 --> 3305.4: regimes, I do think it's
3305.4 --> 3307.3: useful and helpful because that
3307.3 --> 3309.5: becomes a starting point of a reference
3309.5 --> 3311.4: tool that CISOs use,
3311.7 --> 3313.5: that regulators would use, and that
3313.5 --> 3315.6: insurance firms would potentially use
3315.6 --> 3316.2: and turn to.
3317.0 --> 3319.3: They may, of course, pick and choose based on their
3319.3 --> 3319.8: particular
3321.3 --> 3323.4: ecosystem, their particular risk profile,
3323.8 --> 3325.0: but I do agree that
3325.0 --> 3327.4: I know BEGIN isn't an advocacy arm
3327.4 --> 3329.5: but at least as we assess what are the
3329.5 --> 3331.4: right levers that could use and
3332.1 --> 3333.3: operationalize this work,
3333.3 --> 3334.9: I think you're totally right.
3335.2 --> 3337.5: Insurance, even in the
3337.5 --> 3339.4: cyberspace generally, we've seen
3339.4 --> 3341.4: as an opportunity to finally
3341.4 --> 3343.5: be the natural market incentive to
3344.1 --> 3345.7: incentivize good cyber security
3345.7 --> 3347.4: instead of subsidizing poor cyber
3347.4 --> 3347.8: hygiene.
3349.4 --> 3351.4: I think that it would be good to be able to
3351.4 --> 3353.1: give a really good comprehensive
3353.1 --> 3355.3: mapping there and then, of course,
3355.4 --> 3357.1: the benefit of still identifying those gaps.
3357.3 --> 3358.9: I agree with you. I think that insurance
3358.9 --> 3361.5: is a really, really good place for
3361.5 --> 3363.6: regulators and policy makers to turn to.
3370.2 --> 3371.0: So,
3371.2 --> 3372.9: what is our starting point
3373.7 --> 3375.1: to do this mapping?

3378.2 --> 3379.5: To identify
3379.5 --> 3381.1: gaps, we can start from the
3381.1 --> 3382.9: recent acts
3383.8 --> 3385.0: to do
3385.0 --> 3386.5: comprehensive mapping
3387.4 --> 3389.9: different frameworks and controls
3389.9 --> 3391.8: where either we
3391.8 --> 3393.9: start from scratch or we can start from
3395.0 --> 3396.1: your work,
3396.2 --> 3398.1: guys, which is already quite a good input
3398.1 --> 3400.0: because you are going to
3400.0 --> 3402.0: have included
3402.0 --> 3404.0: also already quite a number
3404.0 --> 3405.7: of controls and
3405.7 --> 3406.4: finding
3407.6 --> 3410.0: the other references that correspond to some
3410.0 --> 3412.1: of the controls won't be that hard.
3412.2 --> 3413.8: I mean, depending on what is
3413.8 --> 3415.2: inside, of course, but should be
3416.0 --> 3416.5: feasible.
3420.6 --> 3421.8: I still
3421.8 --> 3423.2: see a value to really
3423.9 --> 3425.8: have somewhere an explanation
3425.8 --> 3426.7: of
3427.7 --> 3429.9: attack paths, attack vectors,
3430.9 --> 3431.0: well,
3432.0 --> 3433.8: known weaknesses
3433.8 --> 3435.2: that have been exploited, maybe
3435.9 --> 3437.7: linking to MITRE ADAPT as well
3437.7 --> 3439.7: because, of course, it's
3439.7 --> 3442.2: well, either ADAPT
3442.2 --> 3444.0: alone or ADAPT
3444.0 --> 3445.7: plus ATT&CK because it's
3445.7 --> 3447.6: really useful to explain
3447.6 --> 3449.0: with standard
3449.6 --> 3451.0: terms, standard vocabulary
3451.6 --> 3453.3: and then to
3454.1 --> 3455.3: maybe to
3455.3 --> 3457.7: highlight what
3457.7 --> 3458.3: was missing
3459.4 --> 3461.7: which also can be
3461.7 --> 3463.4: seen as a contribution to the other
3463.4 --> 3464.9: project from MITRE, different
3465.6 --> 3466.9: in a way
3468.0 --> 3469.4: related to the discussion
3469.4 --> 3471.3: we had yesterday. I think
3471.3 --> 3473.5: it's a way kind of

3473.5 --> 3474.7: to tease
3474.7 --> 3476.8: what we are going
3476.8 --> 3478.5: then to deliver, the
3478.5 --> 3480.7: compressive mapping or
3480.7 --> 3482.6: checklist with respect to all the
3482.6 --> 3484.5: controls and the frameworks
3484.5 --> 3485.4: to be
3486.7 --> 3486.7: followed.
3488.2 --> 3488.5: So,
3490.3 --> 3492.3: question is when do we start
3493.9 --> 3494.5: and
3494.5 --> 3496.0: who is willing to contribute
3496.8 --> 3498.3: because it's always the
3499.1 --> 3500.7: one of the key factors to be
3500.7 --> 3502.1: able to then to deliver something.
3513.8 --> 3514.7: I'd pick
3514.7 --> 3516.6: starting with the highest impact
3516.6 --> 3518.4: areas like that if you wanted to
3518.4 --> 3519.9: start like I guess
3519.9 --> 3521.3: again like
3522.1 --> 3523.9: wherever the greatest value will be
3523.9 --> 3525.8: seen by folks is like looking at
3525.8 --> 3527.6: like what is the current risk picture
3527.6 --> 3528.8: which means generally like
3529.7 --> 3531.6: where is the threat the biggest and
3531.6 --> 3533.5: like what is happening. Basically, where
3533.5 --> 3534.7: are the most common
3534.7 --> 3537.1: the most common attacks and the biggest
3537.1 --> 3539.0: attacks but really the most common attacks
3539.0 --> 3540.8: especially as long as the impact is still
3540.8 --> 3543.0: amounting to a lot like I think that that's
3543.0 --> 3544.7: a good place to start. Generally
3544.7 --> 3546.9: like this is where third party risk
3546.9 --> 3548.6: management and supply chain compromise
3549.6 --> 3550.5: and key
3551.5 --> 3552.8: it's key management and
3552.8 --> 3554.9: compromise and targeting like those
3554.9 --> 3556.8: are some of the places that's where I
3556.8 --> 3558.0: would probably start
3559.2 --> 3561.0: on that. Happily
3561.0 --> 3562.8: that also means you start with a big head
3562.8 --> 3564.6: start not just on traditional
3564.6 --> 3566.7: standards but also where other
3566.7 --> 3568.7: organizations have already mapped
3568.7 --> 3570.2: to specific standards.
3571.0 --> 3572.8: I know some of the challenges I recognize
3572.8 --> 3574.8: the challenge that like anyone who

3574.8 --> 3577.0: has like proprietary standards
3577.0 --> 3578.8: or evaluation frameworks or
3578.8 --> 3580.9: even anything that's trademarked
3580.9 --> 3582.7: because like I don't know what MITRE is doing but
3582.7 --> 3584.1: if I were MITRE I'd be
3584.8 --> 3586.8: like I'd be doing to adapt what I did
3586.8 --> 3588.8: what they did to
3588.8 --> 3590.7: attack which is like you can
3590.7 --> 3592.7: double click and then it'll take you into
3592.7 --> 3594.7: the controls and stuff. They haven't done that yet fo
r adapt
3594.7 --> 3595.9: but like
3595.9 --> 3598.1: that kind of thing
3598.1 --> 3600.8: and ultimately that taxonomy may not be exactly
3600.8 --> 3602.6: what everyone agrees to
3602.6 --> 3604.1: or what Begin agrees to either but
3604.6 --> 3606.6: it's thinking about that sort of framing
3606.6 --> 3608.6: of the vector of attack
3608.6 --> 3610.4: and then the vulnerability
3610.4 --> 3611.9: and the controls
3612.5 --> 3614.7: so it looks similar to even what JFSA
3615.8 --> 3616.6: had started
3616.6 --> 3618.6: to do with their look at several of the
3618.6 --> 3620.1: attacks when they were presenting to us
3620.1 --> 3622.4: on Friday so I think
3622.4 --> 3624.5: it would be something like that
3624.5 --> 3626.5: like you could start that by picking
3626.5 --> 3628.6: a couple of very high impact
3628.6 --> 3630.5: ones that we think would be really valuable
3630.5 --> 3631.1: to industry.
3637.5 --> 3638.5: I'd be willing
3638.5 --> 3640.8: to start that if you want
3640.8 --> 3642.5: I mean I could work with
3642.5 --> 3644.6: somebody and we can get a document going
3644.6 --> 3644.9: out
3644.9 --> 3645.8: I mean
3647.9 --> 3649.2: it has to start somewhere
3649.2 --> 3651.3: right? Someone that's actually knowledgeable
3651.3 --> 3652.6: and sees the landscape
3652.6 --> 3654.7: I mean
3656.1 --> 3657.1: where do we start?
3657.6 --> 3658.9: I mean how do we start it?
3662.0 --> 3663.4: It starts with a document
3663.4 --> 3665.5: and it's a collaborative effort I
3665.5 --> 3667.0: think and it has to be shared knowledge
3667.0 --> 3668.1: right? Yep.
3669.5 --> 3670.6: If I can say

3671.1 --> 3671.6: so
3673.0 --> 3674.0: there's an
3674.0 --> 3675.8: offline key management session
3675.8 --> 3677.7: in the afternoon today
3677.7 --> 3679.8: I believe so I would
3679.8 --> 3682.0: encourage Daniel to
3682.0 --> 3683.9: maybe start that
3683.9 --> 3685.5: conversation because
3686.3 --> 3688.1: Securiosis, the Swiss company
3688.1 --> 3689.8: that he's working with
3689.8 --> 3691.7: that I'm helping promote
3691.7 --> 3693.9: as well, they
3693.9 --> 3695.7: already did a documentation
3695.7 --> 3697.4: for Hong Kong I believe
3697.4 --> 3699.9: so maybe that's also relevant for
3699.9 --> 3701.1: Japan and
3701.7 --> 3703.8: that could be maybe
3703.8 --> 3705.1: a starting point as well
3705.9 --> 3706.9: just a consideration.
3712.4 --> 3713.6: Question, how quickly is
3713.6 --> 3714.8: JFSA going to be publishing
3714.8 --> 3717.4: because if we had a starting point from
3717.4 --> 3719.6: what they had already presented to us
3719.6 --> 3721.4: I don't know did they tell us that? Is
3721.4 --> 3722.9: JFSA here? I don't know.
3723.5 --> 3725.5: No, they told us
3725.5 --> 3725.8: that
3725.8 --> 3727.9: they still
3727.9 --> 3729.7: have some work
3729.7 --> 3731.7: and things to be added but
3731.7 --> 3733.9: you already mentioned and I supported
3733.9 --> 3735.8: this comment that this is already
3735.8 --> 3737.7: good so as
3737.7 --> 3739.7: a first version it would be really good to have
3739.7 --> 3741.7: this document published so maybe we can
3741.7 --> 3742.4: just
3744.9 --> 3745.4: reiterate
3745.4 --> 3746.3: this comment
3746.3 --> 3749.7: just to hope that it will be published
3749.7 --> 3751.7: very soon or maybe it can be shared
3751.7 --> 3753.7: within BEGIN at
3753.7 --> 3755.6: least to frame something on our
3755.6 --> 3756.8: side, to draft something.
3757.8 --> 3759.6: I would like to, you know, today's
3759.6 --> 3761.6: my first day participating in these type of
3761.6 --> 3763.7: discussions, actually I didn't know that this actuall
y

3763.7 --> 3765.8: existed, if I did know I would probably participate
3765.8 --> 3767.6: in it earlier. I did not know about
3767.6 --> 3769.3: JFSA was actually meeting
3769.3 --> 3771.3: last Friday and talking about this
3771.3 --> 3772.5: I would have definitely joined
3773.3 --> 3774.3: but now I do.
3775.9 --> 3777.8: Is there notes from that meeting
3777.8 --> 3779.5: on Friday because I would love to
3779.5 --> 3781.6: read it and see where it needs to
3781.6 --> 3782.8: add to those things.
3785.4 --> 3787.6: So that round table because they
3787.6 --> 3788.4: hosted it
3788.4 --> 3791.6: and they decided
3791.6 --> 3793.2: not to record and things so
3793.2 --> 3795.7: I know we can't
3795.7 --> 3797.5: commit them but I'm also like
3797.5 --> 3799.2: they're speaking this afternoon
3799.2 --> 3801.6: and I assume that some of the other
3801.6 --> 3802.8: members, aren't they
3803.6 --> 3805.0: speaking this afternoon I thought maybe?
3805.9 --> 3807.7: Anyway, we'll connect
3807.7 --> 3809.5: you and I'm positive that they'll have the same
3809.5 --> 3811.4: conversation with you the
3811.4 --> 3813.5: same way that they did with other members of industry.
 They've always been
3813.5 --> 3815.7: really collaborative so then you can
3815.7 --> 3817.4: like probably see in a display
3817.4 --> 3819.5: only way like the slides that
3819.5 --> 3821.4: they showed us because I think you would look
3821.4 --> 3823.5: at that and if you had that
3823.5 --> 3825.4: in front of you right now I think it would
3825.4 --> 3827.4: be clear sort of what we want to build off from.
3828.0 --> 3829.5: Okay. So I'll chat with you offline.
3829.7 --> 3831.4: Oh wonderful. Yeah, no I mean as
3831.4 --> 3833.4: a Japanese citizen and as
3833.4 --> 3835.6: a consumer and as a
3835.6 --> 3837.4: developer and as an enterprise
3837.4 --> 3839.6: I would love to participate
3839.6 --> 3841.8: in drafting this document and
3841.8 --> 3843.4: it's beneficial for me
3843.4 --> 3845.7: not only just from
3845.7 --> 3847.5: a nationalistic point of view but also
3847.5 --> 3849.4: helping at least this industry
3849.4 --> 3851.5: at least from a Japan perspective and hopefully
3851.5 --> 3853.2: it becomes the leading voice in crypto
3853.2 --> 3855.2: and security practices.
3855.8 --> 3857.6: So yeah, whatever I

3857.6 --> 3859.6: can do to help I'll be more than willing to
3859.6 --> 3860.9: offer my assistance.
3862.3 --> 3863.3: Yeah, wonderful.
3864.1 --> 3865.3: I think that's
3865.3 --> 3866.0: first
3867.7 --> 3869.3: action trying to start
3869.3 --> 3871.2: from GFSA study but
3871.2 --> 3873.4: I was wondering maybe you have also
3873.4 --> 3875.7: something within JPCrypto
3875.7 --> 3877.0: ISAC because you analyze
3877.0 --> 3879.2: some of those acts as well
3879.2 --> 3880.9: in order to define
3880.9 --> 3882.2: what needs to be
3883.5 --> 3885.0: emphasized with respect to
3885.0 --> 3887.0: security controls in cloud etc.
3887.2 --> 3889.4: So if you have anything to share that would be very
3889.4 --> 3890.1: helpful as well.
3891.3 --> 3893.4: Okay, so I'll share this later.
3899.6 --> 3900.4: ...
3902.3 --> 3903.0: ...
3903.0 --> 3905.4: at least for this part
3905.4 --> 3907.3: is a way to highlight
3907.3 --> 3908.1: ...
3909.4 --> 3911.4: what happened on those acts
3911.4 --> 3913.2: what has been
3913.2 --> 3914.9: exploited, what is missing
3916.2 --> 3916.9: and
3916.9 --> 3919.1: the second
3919.1 --> 3921.3: action that we can
3921.3 --> 3921.8: do is
3923.1 --> 3923.7: well
3923.7 --> 3925.8: maybe same if you
3925.8 --> 3927.0: can share this checklist
3928.0 --> 3929.9: we can look at it and see
3929.9 --> 3931.8: whether this is a good starting point
3931.8 --> 3934.0: in order to start listing
3934.0 --> 3935.9: controls, mapping
3935.9 --> 3937.9: with frameworks, what needs to
3937.9 --> 3940.0: be added, what can be
3940.0 --> 3940.3: maybe
3941.8 --> 3943.4: well I don't know, updated,
3943.8 --> 3945.9: modified, improved, depending on what
3945.9 --> 3947.8: we see. That's also something
3947.8 --> 3949.5: we can work on.
3949.5 --> 3951.1: And if you have
3951.1 --> 3953.4: an expert member on your side
3953.4 --> 3955.1: willing to contribute that would be even

3956.3 --> 3957.2: more helpful.
3957.4 --> 3959.6: It's really helpful for us because
3959.6 --> 3961.6: our objective is
3961.6 --> 3963.3: to improve this guideline
3963.3 --> 3965.2: by receiving
3965.2 --> 3966.9: your information and so on.
3967.4 --> 3969.2: So as you explained, I think
3969.2 --> 3971.2: this guideline is
3971.2 --> 3972.9: one element and
3972.9 --> 3974.6: to create a map
3975.4 --> 3977.4: is a really important thing
3977.4 --> 3979.0: for beginning and
3979.0 --> 3979.5: itinerary.
3985.3 --> 3985.8: Is
3987.1 --> 3989.2: anybody here, I know I'm looking at Sandra
3989.2 --> 3991.0: because I'm wondering if she's the only one who would know
3991.0 --> 3993.0: anyone here connected to the
3993.0 --> 3995.0: Blockchain Security Standards Council?
3995.5 --> 3997.2: Is there any chance that
3997.2 --> 3999.2: they are doing, I don't actually
3999.2 --> 3999.5: know
4000.4 --> 4003.0: I don't know any of their outputs
4003.0 --> 4005.2: so I don't, like I'm just curious
4005.2 --> 4007.4: if they're a partner to engage
4007.4 --> 4009.4: with, like I've not, I don't know
4009.4 --> 4011.1: what they're working on.
4011.5 --> 4013.1: So I just know it exists is
4013.1 --> 4015.1: basically for the most part all that I know about
4015.1 --> 4016.9: for the most part all that I know about them.
4017.0 --> 4019.0: So if anyone here happens to be familiar
4019.0 --> 4020.9: with them, if they might be a partner
4020.9 --> 4023.1: because there's a chance that they're working on
4023.1 --> 4024.5: this, I don't know,
4025.0 --> 4026.9: maybe not, but I just
4027.7 --> 4028.2: not.
4030.1 --> 4031.2: So there's something
4031.7 --> 4033.0: there's a different group
4033.0 --> 4034.7: but it's related, like it's
4034.7 --> 4036.8: connected, it's like adjacent, there's
4036.8 --> 4038.8: something called the Blockchain Security Standards
4038.8 --> 4040.7: Council. Oh, Mark knows, Mark knows
4040.7 --> 4041.7: everything. Awesome.
4043.1 --> 4044.2: Yeah, if you're okay
4044.2 --> 4045.9: give me a hand to the microphone.
4050.6 --> 4053.0: So they're associated with
4055.3 --> 4056.2: Crypto Isaac

4057.2 --> 4057.8: who's
4058.5 --> 4060.4: Justine Bone who houses it, yeah
4060.4 --> 4060.7: so
4063.3 --> 4063.8: they
4064.3 --> 4065.9: basically just come up on
4065.9 --> 4068.3: the radar with us
4068.3 --> 4070.5: so they are doing a bunch
4070.5 --> 4072.2: of standards, mainly
4073.5 --> 4074.5: all encompassing
4074.5 --> 4076.5: they do do a key management standard
4076.5 --> 4078.2: which happens to be a bit of a copy of
4078.2 --> 4080.4: CCSS, which we always find them
4080.4 --> 4080.7: using.
4082.0 --> 4084.0: They're a membership only
4085.5 --> 4086.0: association
4086.0 --> 4088.4: so you've got to pay, don't quote me on this
4088.4 --> 4090.3: but I think it's about $10,000 to $15,000
4090.3 --> 4092.4: US a year
4092.4 --> 4093.6: to join
4094.1 --> 4096.1: and be part of the chair to help
4096.8 --> 4098.5: these standards. They may be
4098.5 --> 4100.2: interested in
4100.2 --> 4102.3: contributing with this but
4102.3 --> 4103.9: it's pretty much a members only
4104.7 --> 4106.7: standard. It's like PCI DSS
4106.7 --> 4108.3: right, you've got to pay $150,000
4108.3 --> 4110.3: to be at the table to
4110.3 --> 4111.8: contribute to their standards.
4112.3 --> 4114.2: Yeah, they wouldn't meet with us when I was
4114.2 --> 4116.1: in the government, so yeah
4116.1 --> 4117.7: but yeah, sorry Sandra.
4124.6 --> 4125.6: So I think
4125.6 --> 4128.2: based on Mark's comments it sounds like the output
4128.2 --> 4130.2: is not open source, like they keep
4130.2 --> 4132.1: it in house so it's like
4132.7 --> 4134.2: yeah, which I mean
4134.2 --> 4135.3: and there are like
4139.4 --> 4141.6: so they have published some publicly.
4141.8 --> 4143.9: Oh yeah, you can access them, they're absolutely publ
ished
4143.9 --> 4145.8: but if you want to contribute to them you've got to p
ay
4145.8 --> 4147.6: the money. I've only ever seen the
4147.6 --> 4149.7: RECT test from them, so this is neat.
4150.0 --> 4151.7: Okay, then we're going to look at this and see
4151.7 --> 4153.9: which of those will be useful to point to
4153.9 --> 4155.6: so thank you for that because if

4155.6 --> 4157.5: they're already working on something like this
4157.5 --> 4159.8: I couldn't imagine an organisation called
4159.8 --> 4161.1: that not working.
4161.8 --> 4163.8: I mean they're associated with NORS
4163.8 --> 4166.0: as well, you know the node operator
4166.0 --> 4167.2: risk standard.
4167.7 --> 4169.2: They're all in there
4169.9 --> 4170.9: but they're all closed knit.
4172.7 --> 4173.6: So maybe
4173.6 --> 4175.6: we should engage with them.
4175.8 --> 4176.6: Yeah, that's good.
4177.3 --> 4179.4: I mean the key is you want to map
4179.4 --> 4181.5: what's available, right? So if it's open
4181.5 --> 4183.6: source then that's fine. I get
4183.6 --> 4185.5: the contribution part and that's
4185.5 --> 4187.5: close. Yeah, no but that's good news
4187.5 --> 4189.6: actually because that they're publishing
4189.6 --> 4191.6: them publicly because all that I knew of
4191.6 --> 4193.5: that was from I guess
4193.5 --> 4195.7: their intellectual predecessor was
4195.7 --> 4197.6: the RECT test because I don't think they existed
4197.6 --> 4199.7: when they came out with the RECT test but it's
4199.7 --> 4200.6: a lot of the same people
4201.2 --> 4203.7: is my understanding. So like R-E-K-T
4203.7 --> 4205.6: is like a
4205.6 --> 4207.2: high level cyber framework
4207.2 --> 4209.5: so that's cool but that'll be something that
4209.5 --> 4211.5: we should talk to them
4211.5 --> 4213.6: or at least become familiar
4213.6 --> 4215.6: I guess at least try to become familiar
4215.6 --> 4217.4: with their things. Maybe they'll input into
4217.4 --> 4219.4: our process even if they don't want
4219.4 --> 4220.7: us to input into their standards.
4221.7 --> 4223.3: And I wouldn't assume that they
4223.3 --> 4225.7: don't want to talk to us. I'm thinking 3GPP
4225.7 --> 4227.7: which is tens of thousands of dollars
4227.7 --> 4229.8: but they'll invite an expert for
4229.8 --> 4230.1: free.
4231.6 --> 4232.1: Yeah.
4232.8 --> 4235.0: They have at least one standard which is called
4235.0 --> 4236.8: general security and privacy guideline
4236.8 --> 4238.6: where they say that this is mapped with
4238.6 --> 4239.8: NIST CSF.
4244.4 --> 4247.1: So normally I'm shy
4247.1 --> 4249.0: of self-promotion but my whole
4249.0 --> 4250.6: point of being here is to self-promote so
4250.6 --> 4252.7: I will also mention that

4253.3 --> 4255.0: at SEO we're working on
4255.6 --> 4256.8: establishing some form of
4256.8 --> 4258.0: best practices,
4258.5 --> 4259.4: some form of standards
4261.1 --> 4262.7: and I think this is
4262.7 --> 4264.7: also a great opportunity to collaborate.
4265.2 --> 4266.6: I think there's something
4266.6 --> 4268.5: to be said. I've repeated this line a lot of
4268.5 --> 4270.3: times so forgive me if you've heard this before but
4270.3 --> 4272.6: I think despite all of the
4272.6 --> 4274.4: roughness of the crypto ecosystem
4274.4 --> 4275.8: at the end of the day
4275.8 --> 4278.1: among the core developer community
4278.1 --> 4280.4: there is a strong meritocratic nature
4280.4 --> 4282.1: to things where
4282.8 --> 4284.2: it's very hard to get penetration
4284.2 --> 4286.4: when you don't have the respect
4286.4 --> 4288.2: of the builders and the developers who are
4288.2 --> 4290.0: at the end of the day the users
4290.0 --> 4291.9: of what we're trying to build here
4292.2 --> 4293.9: and I think that's somewhere where
4295.2 --> 4296.3: the theory at least
4296.3 --> 4297.6: is that we can leverage
4298.2 --> 4300.2: the reputation that we have through
4300.2 --> 4302.5: initiatives like SEO 911 to then
4302.5 --> 4304.3: tell people, hey, you trusted us
4304.3 --> 4306.2: with this one thing, now we're going to come at
4306.2 --> 4307.6: you with what you would normally
4308.1 --> 4310.4: turn your nose on but in this case
4310.4 --> 4312.5: take our word for it, give it a shot, see if you like
 it.
4315.6 --> 4316.2: Is this
4316.2 --> 4317.5: something that you already started?
4317.9 --> 4319.4: I remember all the
4320.4 --> 4321.7: processes related to
4322.2 --> 4324.1: basically the white hats and how it can
4324.1 --> 4326.3: be managed and how to do it properly
4326.3 --> 4327.9: but I don't remember
4327.9 --> 4329.7: I've seen any action
4329.7 --> 4332.3: yet but it's been a while that I've not
4332.3 --> 4334.1: looked at related to best
4334.1 --> 4335.9: practices for security overall.
4336.7 --> 4337.8: Yeah, so we have two
4337.8 --> 4340.2: separate, we have a two-part approach to this.
4340.3 --> 4342.2: The first is the
4342.2 --> 4344.2: actual standards themselves which are
4344.2 --> 4345.3: open source on GitHub.

4346.1 --> 4347.9: The idea is that anyone can contribute to them
4347.9 --> 4350.1: through a community review
4350.1 --> 4352.0: process and then the second prong
4352.0 --> 4354.1: is the actual enforcement mechanism which
4354.1 --> 4355.1: is how we say, okay,
4357.3 --> 4358.2: the protocols
4358.2 --> 4360.1: that care about security, care about doing
4360.1 --> 4362.1: right by the users, they can just go out there
4362.6 --> 4364.1: follow all the guides
4364.1 --> 4365.9: that we put out, follow all the standards, implement
4365.9 --> 4367.9: all the practices but
4367.9 --> 4369.9: for the protocols that are sort of like
4369.9 --> 4371.8: we will do, we will stick to the
4371.8 --> 4373.7: bare minimum checkbox security
4373.7 --> 4376.2: style then we're going to give you some checkboxes
4376.2 --> 4377.7: and if you tick all
4377.7 --> 4379.7: those off then you achieve this
4380.4 --> 4381.9: baseline or whatever standard
4381.9 --> 4382.8: of security
4383.8 --> 4385.0: but that's sort of like
4386.0 --> 4387.6: the industry kind of runs
4387.6 --> 4389.7: on security seals unfortunately and so we're going to
4389.7 --> 4391.1: give them the security seal.
4394.6 --> 4395.7: That's very good to know
4395.7 --> 4397.9: and we'll have
4397.9 --> 4399.7: to look how we can basically
4399.7 --> 4402.0: make the link bridge between
4402.0 --> 4403.0: those initiatives.
4403.2 --> 4405.9: The goal is not
4405.9 --> 4407.6: to redefine everything and I'm sure
4409.3 --> 4410.0: in the
4410.0 --> 4412.1: best practices you are much more practical
4412.1 --> 4413.1: in terms of
4413.8 --> 4415.9: implementation rather than what we can
4415.9 --> 4417.8: see for instance in this CSF
4418.6 --> 4419.1: so
4419.9 --> 4421.8: trying to map and
4421.8 --> 4423.9: being sure that we explain what can be
4423.9 --> 4425.6: used where would be
4425.6 --> 4426.3: very useful.
4427.5 --> 4429.4: Yeah for sure. I think our focus is
4429.4 --> 4431.2: not strictly to
4431.2 --> 4433.5: recreate or reinvent the
4433.5 --> 4435.4: wheel but rather for things
4435.4 --> 4437.7: that are uniquely crypto native. For example
4437.7 --> 4439.3: a lot of people are
4439.3 --> 4441.5: victimized by account

4441.5 --> 4443.4: takeovers. A protocol has
4443.4 --> 4445.3: a bunch of trusted web properties, their
4445.3 --> 4447.4: Twitter account, their website, their
4447.4 --> 4448.6: YouTube, whatever, their Discord
4449.5 --> 4451.2: and a very crypto native
4451.2 --> 4453.3: way of getting scammed is when that
4453.3 --> 4455.0: protocol loses access to their accounts
4455.0 --> 4457.1: and now it's posting spam links. This doesn't
4457.1 --> 4459.2: happen with YouTube. No one is
4459.2 --> 4460.6: going like, oh my god the
4461.3 --> 4462.9: official YouTube account posted
4462.9 --> 4465.2: on Twitter that the new
4465.2 --> 4467.2: signup form is here, I'm going to sign up and lose
4467.2 --> 4468.8: my YouTube account. That doesn't happen. But in crypt
o
4469.7 --> 4471.3: the project Discord gets
4471.3 --> 4473.2: hacked, they post a spam link
4473.2 --> 4475.3: and $500 million of user
4475.3 --> 4475.8: funds are gone.
4477.8 --> 4479.1: An example of something that I think
4479.1 --> 4481.2: would be very hard to get upstreamed into
4481.2 --> 4483.1: ISO or into Socktree or
4483.1 --> 4485.0: whatever is how do you secure
4485.0 --> 4486.0: your Twitter account?
4486.7 --> 4488.8: That's something that I think we have more
4489.5 --> 4491.2: flexibility to cover. But definitely
4491.2 --> 4493.0: not trying to reinvent the wheel on other things
4493.0 --> 4495.2: especially Web 2.0 things that
4495.2 --> 4496.7: are already very well enumerated.
4497.3 --> 4498.6: I think that's where we're hoping
4499.2 --> 4501.0: with the second prong to say
4501.0 --> 4503.0: okay, if you want the
4503.0 --> 4505.1: crypto native seal, the crypto
4505.1 --> 4507.1: native checkboxes, go to this other thing
4507.1 --> 4507.9: that already exists,
4508.9 --> 4510.1: fill all those requirements
4510.1 --> 4511.9: and we will say
4511.9 --> 4514.3: with our reputation that you
4514.3 --> 4516.1: have met the baseline requirements
4516.1 --> 4518.2: for security in crypto. But really all
4518.2 --> 4520.5: you have to do is do the thing that already exists.
4520.6 --> 4522.3: Great, the trad cert, I like it.
4522.5 --> 4523.6: I'm kidding, I'm sorry.
4526.5 --> 4528.2: Agreed, agreed. And then that
4528.2 --> 4530.0: would allow for the people who have really
4530.7 --> 4532.2: good understanding of the unique
4532.9 --> 4534.1: implementations for Web 3.0 to

4534.1 --> 4536.3: focus where those big gaps are. I think
4536.3 --> 4538.2: that's awesome. Cool,
4538.4 --> 4540.2: okay, that's good. Then
4540.2 --> 4542.2: we'll reach out to
4542.7 --> 4543.9: BSSC and see if
4544.6 --> 4546.0: they're open to chatting.
4552.3 --> 4554.2: Actually, sorry, quick question to
4554.2 --> 4556.2: Sandra. I know
4556.2 --> 4558.4: you guys are doing work on cyber security.
4558.6 --> 4560.2: I realize I don't know exactly what
4560.2 --> 4561.9: it is that you're doing. Would you be willing to shar
e?
4562.3 --> 4564.1: I know it's still forming.
4566.6 --> 4568.5: We have a multi-layer
4568.5 --> 4569.9: approach, so phase one
4569.9 --> 4572.3: includes cyber security related
4572.3 --> 4574.2: risk frameworks and mitigants.
4574.6 --> 4576.0: Not controls, but
4576.0 --> 4578.2: mitigations. That is
4578.2 --> 4580.1: really from the point of view of regulated
4580.1 --> 4582.1: financial institutions and how they would deal
4582.1 --> 4584.6: with basically
4584.6 --> 4585.9: building new
4585.9 --> 4588.2: risks that are novel risks
4588.2 --> 4590.3: that are identified using particularly
4590.3 --> 4592.2: public blockchains into
4592.2 --> 4594.4: their existing risk framework. So it's a very
4594.4 --> 4596.1: specific point of view,
4596.4 --> 4598.3: but the
4598.3 --> 4599.5: first layer that we
4600.4 --> 4602.4: released, it's public domain.
4603.1 --> 4604.1: It was July
4604.1 --> 4606.2: 2025. That version focused
4606.2 --> 4607.3: on tokenized securities.
4607.8 --> 4610.1: The next version comes out in a
4610.1 --> 4612.0: couple weeks, which is an extension into
4612.0 --> 4612.7: L2
4613.6 --> 4615.6: risk mitigants, and then
4615.6 --> 4618.3: we have kicked off phase two
4618.3 --> 4619.9: on-chain digital payments,
4620.1 --> 4621.7: which cover stablecoin
4621.7 --> 4623.7: and deposit tokens
4623.7 --> 4625.4: and tokenized deposits,
4625.8 --> 4628.0: which are two separate things, and then
4628.0 --> 4629.6: eventually we'll get to CBDC.
4630.6 --> 4631.8: The third layer,
4631.9 --> 4633.8: which is this layer, is

4633.8 --> 4635.6: crypto assets. I think
4635.6 --> 4637.7: what we're going to do is when we get
4637.7 --> 4639.6: to that towards the end of the year, is
4639.6 --> 4641.9: take a look at the work that you all have done,
4642.5 --> 4643.4: canvas the market,
4644.1 --> 4645.6: and then see what we can build
4645.6 --> 4648.0: in, because we're not interested in reinventing
4648.0 --> 4649.4: the wheel. If people have done it,
4649.4 --> 4651.4: we're happy to integrate it, but it's
4651.4 --> 4653.6: from the point of view of regulated financial
4653.6 --> 4654.6: institutions.
4659.8 --> 4661.5: The answer to the person in chat is
4661.5 --> 4661.8: yes.
4669.1 --> 4669.7: Perfect.
4671.6 --> 4672.1: Perfect.
4673.1 --> 4674.1: Thank you.
4675.3 --> 4677.0: I think we are good.
4677.0 --> 4678.1: We will
4679.7 --> 4680.8: probably need
4680.8 --> 4682.0: a few
4683.1 --> 4684.9: remote sessions to start
4684.9 --> 4686.5: the groundwork, but
4686.5 --> 4688.5: we have quite a good
4689.2 --> 4690.7: idea of what needs to be done.
4691.0 --> 4692.9: Thanks, everyone. That was a very
4693.5 --> 4695.1: productive session. Thank you.
4696.1 --> 4697.1: I think
4697.1 --> 4699.1: we break for about one hour,
4699.4 --> 4701.0: and then after that, if I
4701.0 --> 4702.7: remember correctly, I don't have the schedule
4704.2 --> 4705.1: with me, but
4705.1 --> 4706.1: I think we have
4707.3 --> 4708.3: a presentation
4709.2 --> 4709.7: from
4712.1 --> 4712.6: maybe
4712.6 --> 4714.7: GFSA. Yes, you're right, Carol.
4714.9 --> 4716.6: Maybe this is from GFSA,
4716.8 --> 4718.6: and then after that, around
4720.0 --> 4720.9: 2.30
4720.9 --> 4722.6: or something like this, or maybe
4722.6 --> 4724.5: around 2, we have the session on
4724.5 --> 4725.5: key management.
4727.6 --> 4728.9: I'm so sorry, because I know
4728.9 --> 4730.1: you just convened everybody,
4731.0 --> 4732.5: whatever, just missed everyone, but
4732.5 --> 4733.6: since everyone's still here,
4734.9 --> 4736.6: given the NIST workshop

4736.6 --> 4738.7: in April that they talked about,
4739.5 --> 4740.7: they mentioned it yesterday
4740.7 --> 4742.6: that there's going to be a NIST workshop on April
4742.6 --> 4744.4: 16th, whatever, around that.
4744.5 --> 4745.5: Yes, 16th.
4748.0 --> 4748.8: I know
4748.8 --> 4750.4: we must be
4750.4 --> 4752.1: and will be thinking about
4752.1 --> 4754.3: what is it that we hope
4754.3 --> 4756.6: that we can try to help get out of
4756.6 --> 4758.0: this workshop. Now,
4758.3 --> 4759.7: NIST is setting their agenda,
4759.7 --> 4761.2: but ultimately,
4762.3 --> 4763.9: part of where BEGIN
4763.9 --> 4766.2: can be thinking is about where we want to be making
4766.7 --> 4768.0: recommendations or suggestions
4768.0 --> 4770.1: to get, obviously NIST has been participating
4770.1 --> 4771.7: in both sides
4772.3 --> 4773.6: of the room in different ways
4773.6 --> 4775.9: throughout all of this, but if there's specific
4775.9 --> 4778.1: work where we want, where we feel
4778.1 --> 4780.0: that even NIST convening would be
4780.0 --> 4780.5: useful,
4781.8 --> 4783.8: and maybe the right answer is that that comes later,
4784.0 --> 4786.1: but some of this feels very much
4786.1 --> 4787.9: like what Cyber went through when we were
4787.9 --> 4789.7: creating the NVD, that
4789.7 --> 4792.0: when we were creating the National Vulnerability Data
base,
4792.2 --> 4793.8: trying to come up with a structured approach
4793.8 --> 4795.8: for thinking about how to define what
4795.8 --> 4797.8: is a CVE and how
4797.8 --> 4799.5: you want to discuss both
4799.5 --> 4801.9: threat and the vulnerability,
4802.2 --> 4803.7: the issue that's being exploited,
4803.8 --> 4805.4: but then also the control that would have
4805.9 --> 4807.6: patched the vulnerability that would have
4807.6 --> 4809.6: defeated the attack vector.
4811.8 --> 4813.5: In fact, we're going to talk to you
4813.5 --> 4815.7: and anybody maybe at NIST and
4815.7 --> 4817.4: MITRE about how we
4817.4 --> 4819.5: should best structure literally
4819.5 --> 4821.4: just the documentation to start thinking
4821.4 --> 4823.5: through this. I think using a framework
4823.5 --> 4825.6: like that feels right to me,
4825.9 --> 4827.6: but I'm a cyber nerd, so of course I feel
4827.6 --> 4829.2: like the NVD framework feels like

4829.2 --> 4831.6: a good framework, so that may not
4831.6 --> 4833.5: be the best one, but I at least think
4833.5 --> 4835.4: that that's an idea of something that Begin
4835.4 --> 4837.3: could go into that workshop
4838.3 --> 4839.5: with an agenda of
4839.5 --> 4841.5: trying to say, hey, maybe this is a good
4841.5 --> 4843.4: idea. I'm sure that we feel that way
4843.4 --> 4845.4: in lots of other work streams, though, so we can deci
de
4845.4 --> 4847.4: what the different priorities are of what we want to
be
4847.4 --> 4849.5: pitching in that NIST meeting.
4857.0 --> 4859.0: Thank you, everyone. Enjoy your lunch.
4902.1 --> 4902.9: Thank you.
4919.0 --> 4921.8: Thank you.
4935.3 --> 4936.1: Thank you.