BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

In the Matter of the Joint Application of Sprint Communications Company L.P. (U-5122) and T-Mobile USA, Inc., a Delaware Corporation, for Approval of a Transfer of Control of Sprint Communications Company L.P. Pursuant to California Public Utilities Code Section 854(a).	Application 18-07-011 (Filed July 13, 2018)
And Related Matters.	Application 18-07-012 (Filed July 13, 2018)

ATTACHMENT C: SUPPLEMENTAL
DECLARATION OF KRISTINA DONNELLY
OF THE PUBLIC ADVOCATES OFFICE

(Public Version)

April 26, 2019

TABLE OF CONTENTS

LIST OF ATTACHMENTS

Attachment 1: Statement of Qualifications

Attachment 2: TISS-610: Enterprise Third-Party (Supplier) Information Security Standard, T-Mobile Supplemental Response to Public Advocates Office DR 004, Attachment Titled "TMUS-CPUC-PA-00005629.Public_Enterprise Third-Party Information.pdf"

Attachment 3: TRS-610: Enterprise Third-Party (Supplier) Risk Management Standard, T-Mobile Supplemental Response to Public Advocates Office DR 004, Attachment Titled "TMUS-CPUC-PA-13000088(PUBLIC).pdf"

Attachment 4: Cyber Assessment Questionnaire, T-Mobile Supplemental Response to Public Advocates Office DR 004, Confidential Attachment Titled "TMUS-CPUC-PA-00005641.Confidential.xlsx"

Attachment 5: Supplier Risk Management (SRM) Questionnaire, T-Mobile Supplemental Response to Public Advocates Office DR 004, Confidential Attachment Titled "TMUS-CPUC-PA-00005642.Confidential.xlsm"

Attachment 6: "TLP-500 Customer Location Information Policy," T-Mobile Supplemental Response to Public Advocates Office DR 004, Confidential Attachment Titled "TMUS-CPUC-PA-00005626.Confidential_customer Location information policy.pdf"

Attachment 7: T-Mobile Response to Public Advocates Office Data Request 007, Questions 7-10, 7-12, and 7-13

Attachment 8: T-Mobile Supplemental Response to Public Advocates Office Data Request 010, Questions 10-8, 10-14, and 10-15

I. EXECUTIVE SUMMARY

1. This Supplemental Declaration responds to new evidence and arguments raised in the January 29, 2019 Rebuttal Testimony of Ms. Susan Brye from T-Mobile and summarizes the potential impact of the proposed transaction on consumer privacy and data security. Specifically, this Supplemental Declaration evaluates T-Mobile's policies and practices for ensuring privacy and data security when allowing third-parties to access or use non-public T-Mobile confidential information, including customer data.

2. In my Direct Testimony, I evaluated T-Mobile's Third-Party Risk Management (TPRM) program and practices and concluded that the TPRM program and practices contain important gaps that put customers at risk. The Rebuttal Testimony provided by Ms. Brye provides evidence purporting that T-Mobile's TPRM program is thorough and robust; however, the information T-Mobile has provided does not support this claim. Therefore, I conclude that T-Mobile has failed to demonstrate their practices are sufficient for the merger to be in the public interest. In light of this conclusion, as well as all of the evidence provided by the Pubic Advocates Office over the course of this proceeding, the Commission should deny the merger.

II. INTRODUCTION

3. The February 26, 2019 Administrative Law Judge's Ruling Denying in Part and Granting in Part the Motion of the Public Advocates Office to Amend and Supplement Testimony and for Additional Hearings; and Revising the Schedule of this Proceeding (ALJ Ruling) directed the Public Advocates Office to respond to new evidence and arguments raised in the Rebuttal Testimony of Sprint and T-Mobile (Applicants).

4. As discussed in my Direct Testimony, both T-Mobile and Sprint have experienced customer data privacy breaches that resulted from third-party

supplier access to their customers' data.[1] Since then, reports continue to emerge[2] detailing how a variety of actors – including bounty hunters, bail bondsman, stalkers, and domestic abusers – have purchased or accessed wireless customer location data through the wireless companies' (including Sprint and T-Mobile[3]) third- and fourth-party suppliers. Some actors were even able to obtain highly-accurate customer location information, even though federal regulation explicitly prohibits carriers from using these data for any purpose other than emergency response.[4]

5. Protecting access to customer information is necessarily more difficult when the data are accessed and used by non-affiliated companies. Considering that reports have exposed numerous and different ways that sensitive wireless customer information has been accessed and sold by third- and fourth-party suppliers, wireless carriers have a particularly important responsibility to thoroughly review these engagements, and to employ strong contracts with monitoring requirements that enable the carriers to ensure their customers' data are protected.

---

[1] Public Advocates Office Testimony on Privacy by Kristina Donnelly (Donnelly Direct Testimony) at pp. 6-7.

[2] Cox, Joseph. Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years. *Motherboard.* February 6. Accessed: March 25, 2019. https://motherboard.vice.com/en_us/article/43z3dn/hundreds-bounty-hunters-att-tmobile-sprint-customer-location-data-years.

[3] Cox, Joseph. T-Mobile Reveals More Location Data Abuse Following Questions from Senator Wyden. *Motherboard.* March 13, 2019. Accessed: March 25, 2019. https://motherboard.vice.com/en_us/article/d3mjvy/tmobile-phone-location-data-abuse-senator-ron-wyden.

[4] Cox, Joseph. What A-GPS Data Is (and Why Wireless Carriers Most Definitely Shouldn't Be Selling It). *Motherboard.* February 7, 2019. Accessed: March 25, 2019. https://motherboard.vice.com/en_us/article/j575dg/what-a-gps-data-is-and-why-wireless-carriers-most-definitely-shouldnt-be-selling-it.

III. ANALYSIS

6. In the Rebuttal Testimony of Ms. Susan Brye, T-Mobile introduces new evidence regarding its program for managing the risks posed by third party supplier access to T-Mobile confidential information, including customers' personal information. This Supplemental Declaration evaluates this new information and re-assesses my previous analysis of this risk.

7. This document refers to a number of similarly-named T-Mobile documents; for the reader's reference, these documents are summarized as follows:

- **Enterprise Third-Party (Supplier) Information Security Standard (New TISS-610):**[5,6] This Standard "define(s) T-Mobile's third-party information security requirements that help meet T-Mobile's overall risk management and security objectives."[7] TISS-610 applies to all suppliers, including those that access, host, retain, process, or transmit non-public T-Mobile information.[8] To help the reader differentiate among similarly-named documents, this Supplemental Declaration refers to this document as "New TISS-610."
- **TRS-610 Enterprise Third-Party (Supplier) Risk Management Standard (Legacy TRS-610):**[9] TRS-610 is a legacy version of TISS-610 and was replaced by New TISS-610 during the first week of December 2018.[10] To help the reader differentiate these two documents, I refer to TRS-610 as "Legacy TRS-610".
- **Exhibit B:**[11] Exhibit B is a data security template that T-Mobile uses to establish suppliers' obligations to maintain the security of T-Mobile's

[5] Donnelly Direct Testimony, Exhibit D-2.

[6] TISS-610 is also included here as Attachment 2.

[7] Attachment 2: TISS-610 at section 1.

[8] Attachment 2: TISS-610 at section 2.1.

[9] Attachment 3: TRS-610.

[10] Donnelly Direct Testimony, Exhibit D-1.

[11] Brye Rebuttal Testimony, Attachment A.

confidential information, which includes customer data.[12] T-Mobile includes this template as part of suppliers' master service agreements when the supplier has access to T-Mobile's confidential information.

- **Cyber Assessment Questionnaire (New Cyber Assessment):**[13],[14] The Cyber Assessment Questionnaire is an excel-based cyber security and data handing review questionnaire that all third-parties with access to T-Mobile confidential information must complete as part of their initial review process. T-Mobile recently updated this assessment; however, the company submitted contradictory information regarding when they began using this new version.[15] To help the reader differentiate among similarly-named documents, this Supplemental Declaration refers to this questionnaire as the "New Cyber Assessment."

- **Supplier Risk Management Review (SRMR):** The SRMR is the legacy version of the New Cyber Assessment.[16] To complete the SRMR, "Suppliers provide a self-attestation via T-Mobile's Supplier Risk Management (SRM) questionnaire, third party independent audit reports (if available), and other supporting documents as requested. The SRMR is a desk review of those documents."[17]

- **Supplier Risk Management (SRM) Questionnaire (Legacy SRM Questionnaire):**[18],[19] The Legacy SRM Questionnaire is a macro-enabled

[12] Brye Rebuttal Testimony at p. 8: 22-27.

[13] Donnelly Direct Testimony, Exhibit D-5.

[14] For the reader's benefit, a pdf version of the Cyber Assessment is also included here, as Attachment 4. Although T-Mobile originally submitted the New Cyber Assessment as an Excel workbook, I have created a pdf for inclusion in this Supplemental Declaration. The name of each tab of the workbook appears at the top of the page.

[15] According to T-Mobile's response to Data Request 004 dated December 21, 2018, the New Cyber Assessment went into production in early October 2018, and entirely replaced the Supplier Risk Management Review (SRMR) in November 2018 (See Donnelly Direct Testimony, Exhibit D-1). However, T-Mobile's Supplemental Response to DR 010 dated April 5th, 2019 states that the New Cyber Assessment went into effect in July 2018 (see Attachment 8: Responses to DR 10-14 and 10-15).

[16] Brye Rebuttal Testimony at p. 7: 10-19.

[17] Attachment 3: TRS-610.

[18] Attachment 5: Supplier Risk Management (SRM) Questionnaire.

[19] Although T-Mobile originally submitted the Legacy SRM Questionnaire as a macro-enabled Excel workbook, I have created a pdf for inclusion in this Supplemental Declaration. The name of each tab of the workbook appears at the top of the page.

excel workbook that was one component of the SRMR. The SRM Questionnaire is comprised of an intake screening form (which is completed by T-Mobile staff) and a cybersecurity questionnaire (which is completed by the supplier).[20] According to T-Mobile, the New Cyber Assessment replaced the Legacy SRM Questionnaire in either July 2018 or November 2018.[21,22]

- **Customer Location Information Policy (TLP-500)**:[23] This policy **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]**

8. Readers should also note that, in this Supplemental Declaration, I use the terms "third-party" and "supplier" interchangeably. In addition, "subcontractor" refers to a supplier's own third-party relationships; as discussed in my Direct Testimony, the industry sometimes refers to these as "Nth party" relationships.

A. T-Mobile's New Third-Party Risk Management Program Has Gaps That Put Customer Data At Risk.

9. In my Direct Testimony, I concluded that T-Mobile's third-party review process likely contains some significant gaps. Ms. Brye's Rebuttal Testimony attempts to assuage these concerns, stating that the TPRM Program is "established, comprehensive and robust."[24] She goes on to say, "although we are continuously improving and recalibrating the TPRM Program to reflect changing business needs, our program is comprehensive and particularly robust."[25] Ms. Brye describes the recent "recalibration" of the TPRM program,

[20] Brye Rebuttal Testimony at p. 7: 10-13.

[21] Attachment 8: T-Mobile Response to DR 010 Questions 10-14 and 10-15.

[22] Donnelly Direct Testimony, Exhibit D-1.

[23] Attachment 6: TLP-500 Customer Location Information Policy.

[24] Brye Rebuttal Testimony at p. 3: 5-6.

[25] Brye Rebuttal Testimony at p. 3: 14-16.

stating that, relative to the legacy program, the new TPRM program is "even more comprehensive" and that New TISS-610 "better aligns with [National Institute of Standards and Technology] NIST standards, technology advancements, and security industry best practices."[26]

10. However, neither Ms. Brye's Testimony nor T-Mobile's Data Request (DR) responses sufficiently address multiple concerns about T-Mobile's programs and processes for managing third-party risks. The recent revisions to the program suggest the most recent recalibration process has introduced errors and gaps that could make it more challenging for suppliers to complete the TPRM review process and comply with T-Mobile's requirements, which could ultimately put T-Mobile customers at risk. In this section, I describe a few ways that T-Mobile's new TPRM program is not as "established, comprehensive and robust" as the legacy program.

1. New TISS-610 Does Not "Better Align" with NIST Standards, Technology Advancements, Or Security Industry Best Practices.

11. In response to Ms. Brye's statements about the New TISS-610, the Public Advocates Office asked T-Mobile to describe "all of the specific changes that were made between the previous TRS-610 program and the new TISS-610, and how they better align the TPRM program with NIST standards, technology advancements, and security industry best practices."[27] T-Mobile provided the following response:[28]

"The two policies are very similar in substance; however, new TISS-610 released to improve readability and present T-Mobile's supplier security requirements in a more accessible and understandable format (e.g., plain language in a T-Mobile "Uncarrier" format). Additionally, the security domains covered in that policy were reordered and

[26] Brye Rebuttal Testimony at p. 7: 6-20.

[27] Brye Rebuttal Testimony at p. 7: 19-20.

[28] Attachment 8: T-Mobile Response to DR 010 Question 10-15.

are now presented in the same order as questions the supplier must complete under the new TPRM Cyber Assessment that went into effect in July 2018. Suppliers can now better track T-Mobile's cyber security requirements in line with the questions/information T-Mobile seeks in that assessment, thereby reducing questions and facilitating the supplier's clearer understanding of T-Mobile's requirements for access to non-public data."

12. This statement is problematic for three reasons.

13. First, this response clearly shows that Ms. Brye's statement that the New TISS-610 "better aligns with NIST standards, technology advancements, and security industry best practices," is false since, according to T-Mobile, the only differences between the two documents relate to their organization and format, and not to their substance.

14. Second, T-Mobile incorrectly states that the security domains covered in TISS-610 "are now presented in the same order as questions the supplier must complete under the new TPRM Cyber Assessment." A comparison of the contents of New TISS-610 to the questions contained in the New Cyber Assessment shows that this is simply not the case. **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]**

15. Third, some of the cyber security requirements outlined in New TISS-610 are missing from the New Cyber Assessment. For example, **[BEGIN CONFIDENTIAL]** [redacted]

[redacted] **[END CONFIDENTIAL]**

16. T-Mobile asserts that the recent changes to New TISS-610 allow suppliers to "better track T-Mobile's cyber security requirements in line with the questions/information T-Mobile seeks in that assessment" and "facilitate the supplier's clearer understanding of T-Mobile's requirements for access to non-public data." However, suppliers might not find the information easier to track considering the information contained in the two documents cannot be quickly or easily aligned. More importantly, the changes do not appear to facilitate clearer understanding of T-Mobile's requirements, since some of the requirements in New TISS-610 are not reflected in the questions in the New Cyber Assessment. Therefore, we cannot conclude that T-Mobile's recent recalibration of the TPRM program is "comprehensive" or "particularly robust."

2. The New Cyber Assessment Lacks Important Guidance and Contains Obvious Errors and Omissions.

17. Additional evidence suggests that the New Cyber Assessment also contains gaps. As stated previously, T-Mobile uses the Cyber Assessment to evaluate supplier's cyber security and data handing practices; all third-parties with access to T-Mobile confidential information must complete the Assessment during T-Mobile's initial review of the supplier and then periodically thereafter. T-Mobile recently implemented a new version of this assessment; however, it is not clear how long the New Cyber Assessment has been in use because T-Mobile has submitted contradictory information regarding when they

implemented the new version.[29] Regardless, the New Cyber Assessment clearly contains gaps and errors, and may not ultimately be an improvement over the legacy version that it replaced.

18. The Legacy SRM Questionnaire is a macro-enabled Excel workbook that contains **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]**

19. On the other hand, the New Cyber Assessment is a standard excel workbook and is far less user-friendly than the Legacy SRM Questionnaire. The New Cyber Assessment **[BEGIN CONFIDENTIAL]** [redacted]

[29] According to T-Mobile's response to DR 004 dated December 21, 2018, the New Cyber Assessment went into production in early October 2018, and entirely replaced the Supplier Risk Management Review (SRMR) in November 2018 (See Donnelly Direct Testimony, Exhibit D-1). However, T-Mobile's Supplemental response to DR 010 dated April 5th, 2019 states that the New Cyber Assessment went into effect in July 2018 (see Attachment 8: T-Mobile Response to DR 010 Questions 10-14 and 10-15).

[redacted]

20. [redacted]

[END CONFIDENTIAL]

21. As stated previously, T-Mobile claims the recent changes to the TPRM program materials, including the Cyber Assessment, would "[facilitate] the supplier's clearer understanding of T-Mobile's requirements for access to non-public data."[30] However, the New Cyber Assessment is clearly *less* effective at communicating T-Mobile's requirements than the legacy version that it replaced. Any changes to T-Mobile's TPRM program should help suppliers complete these important assessments more easily; however, these changes make the process more opaque. This is important since any new suppliers – particularly those that T-Mobile may inherit from Sprint – will likely find it challenging to both understand their requirements and complete the Assessment. The fact that the New Cyber Assessment is far less user-friendly than the legacy version and contains numerous errors suggests that T-Mobile

[30] Attachment 8: T-Mobile Response to DR 010 Question 10-15.

has not implemented the New Cyber Assessment thoroughly or carefully, and these changes may introduce gaps in T-Mobile's awareness of, and ability to control, data security threats stemming from its third-party relationships.

3. T-Mobile's TPRM Materials Contain Inconsistent And Conflicting Terminology.

22. The New Cyber Assessment, the New TISS-610, Ms. Brye's Rebuttal Testimony, and T-Mobile's DR responses contain numerous inconsistent and conflicting references to T-Mobile departments and forms. These inconsistencies suggest that T-Mobile did not implement the recent programmatic changes to the TPRM program thoroughly or carefully, and may confuse suppliers, particularly those T-Mobile may acquire from Sprint as a result of this merger, since new suppliers will not be as familiar with T-Mobile's processes or organization.

23. In her Rebuttal Testimony, Ms. Brye refers to her program as the "TPRM Program" and states that TPRM's review includes, among other assessments, the New Cyber Assessment.[31] However, New TISS-610 states that T-Mobile's Supplier Cyber Risk Management (SCRM) Team "performs detailed Cyber Assessments."[32] So, even though the TPRM Program and the SCRM Team have either overlapping or duplicative responsibilities to implement and review the Cyber Assessment, Ms. Brye does not mention the SCRM Team, and does not describe whether or how the TPRM Program she directs coordinates with the SCRM Team to assess and manage the risk of third-party access to T-Mobile confidential information.

[31] Brye Rebuttal Testimony at p. 3: 23.

[32] Attachment 2: TISS-610 at section 3.2.

24. In addition, New TISS-610 states that it is "aligned to the Enterprise (Supplier) Risk Management Program" (ESRAP).[33] The ESRAP is not mentioned in either Ms. Brye's Rebuttal Testimony or any of T-Mobile's DR responses. If the ESRAP is an existing program that manages T-Mobile's supplier risks (as the name suggests), then I would have expected that T-Mobile would have made at least one, if not numerous, references to the program in their DR responses and in Rebuttal Testimony; however, they did not mention this program at all.[34]

25. New TISS-610 also states, "T-Mobile will complete an Enterprise (Supplier) Risk Management Program (ESRAP) intake for all Suppliers."[35] However, T-Mobile claims,[36] and Ms. Brye's Rebuttal Testimony repeats,[37] that the intake screening form had been part of the Legacy SRM Questionnaire and is therefore no longer in use.[38] The New Cyber Assessment only contains questions addressed to the supplier and not to T-Mobile staff, so it also does not contain the intake screening form.[39] The Public Advocates Office asked T-Mobile to provide details about *all* of T-Mobile's supplier risk assessments and who is responsible for completing and reviewing them;[40] however, T-Mobile did not describe or provide a copy of any intake screening form.

26. T-Mobile's response[41] to our question regarding T-Mobile's supplier risk assessments introduces additional confusion about the company's process for

[33] Attachment 2: TISS-610 at sections 1 and 3.2.

[34] Helpfully, Legacy TRS-610 outlined previous changes T-Mobile made to the names of different forms and departments (sections 1 and 2.1 sub-section 19), but T-Mobile did not include similar information in New TISS-610.

[35] Attachment 2: TISS-610 at section 1.

[36] Donnelly Direct Testimony, Exhibit D-1.

[37] Brye Rebuttal Testimony at p. 7: 6-20.

[38] Attachment 5: Legacy SRM Questionnaire at pp. 6-7.

[39] Attachment 4: Cyber Assessment Questionnaire.

[40] Attachment 8: T-Mobile Response to DR 010 Question 10-8.

[41] Attachment 8: T-Mobile Response to DR 010 Question 10-8.

reviewing completed assessments. T-Mobile's response states that, "TPRM analysts have primary responsibility for reviewing non-cyber assessments. Analysts on the Supplier Cyber Risk Management team within the Digital Security Office have primary responsibility for reviewing Cyber Assessments."[42] Not only does this statement conflict with Ms. Brye's single reference to a "Digital Security *Organization*"[43] (not *Office*), it directly contradicts her assertion that the TPRM team is responsible for administering and reviewing the Cyber Assessment.[44] It also conflicts with T-Mobile's response to an earlier DR, which stated, "the TPRM Program has ultimate oversight and strategic responsibility for the supplier assessment processes, including the Cyber Assessment."[45]

27. An "established" program would not rely on key documents that contain errors and inconsistencies. Moreover, T-Mobile's DR responses to questions about the program would not contain errors and inconsistencies if the program were truly "established." Therefore, I conclude that T-Mobile's TPRM program may contain gaps that put customers at risk.

4. TPRM's Policy Documents Are Missing, or Inconsistently Describe, Important Supplier Requirements.

28. Ms. Brye is incorrect when she claims that the TPRM program is "comprehensive" and "robust" because T-Mobile's policy and contractual documents omit or inconsistently describe some important requirements that are included in the New Cyber Assessment. This may cause confusion for T-Mobile's suppliers.

---

[42] Attachment 8: T-Mobile Response to DR 010 Question 10-8.

[43] Brye Rebuttal Testimony at p. 6: 26.

[44] Brye Rebuttal Testimony at p. 3: 23-27.

[45] Attachment 7: T-Mobile Response to DR 007 Question 7-10.

29. For example, **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** This inconsistency would not exist in a truly comprehensive and robust program.

30. In addition, **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]**

31. Removing this language from TISS-610 obfuscates suppliers' contractual obligations and makes it more difficult for suppliers to understand and ensure their compliance with T-Mobile's expectations. This is counter to the stated intent of T-Mobile's revisions to New TISS-610, which are to "[facilitate] the supplier's clearer understanding of T-Mobile's requirements for access to non-public data."[46]

32. Relevant language is also not included in Exhibit B, where **[BEGIN CONFIDENTIAL]** [redacted]

[46] Attachment 8: T-Mobile Response to DR 010 Question 10-15.

[redacted] **[END CONFIDENTIAL]**

33. I would expect T-Mobile to outline *all* supplier requirements in its policy documents (i.e. the New TISS-610) and/or in Exhibit B, which is part of a supplier's master service agreement and establishes a supplier's specific obligations to maintain the security of T-Mobile confidential information. **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** However, the New Cyber Assessment is not a "policy" – it is an assessment that provides T-Mobile a snapshot of a supplier's cybersecurity practices at a single point in time; no T-Mobile document states or suggests that suppliers must adhere to the requirements described in the New Cyber Assessment. New TISS-610 states that the "Supplier is responsible for completing cyber (*sic)* assessment questionnaire and adhering the (*sic*) security requirements in this Standard."[47] Therefore, New TISS-610 does not require suppliers to adhere to the requirements outlined in the New Cyber Assessment; it only requires that they complete it.

34. As a result, T-Mobile's new TPRM Program does not appear to be as robust or comprehensive as the legacy version.

[47] Attachment 2: TISS-610 at section 3.1.

B. T-Mobile's Customer Location Information Policy Puts Customers At Risk.

35. Ms. Brye's repeated assertions[48] regarding the comprehensiveness of the TPRM program are further undermined by the fact that T-Mobile's policies omit some important and relevant requirements regarding the handling of customer location information. This issue is a particularly important issue in light of the recent allegations described in the Introduction Section of this Supplemental Declaration, which describes how wireless carriers have been improperly providing access to or selling their customers' location information.

36. T-Mobile's Customer Location Information Policy (TLP-500)[49] **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]**

37. However, **[BEGIN CONFIDENTIAL]** [redacted] **[END CONFIDENTIAL]** In 2015, the Federal Communications Commission (FCC) issued regulations governing the use of highly-accurate location information that they require carriers to collect and provide to emergency responders, when needed. The regulations state, in no uncertain terms, that this highly-accurate location information may only be used

[48] Brye Rebuttal Testimony at p. 3: 5-7 and 13; and p. 7: 16-19.

[49] Attachment 6: TLP-500.

"to respond to the user's call for emergency services," and carriers are expressly not allowed to use the data for any other purpose.[50]

38. **[BEGIN CONFIDENTIAL]** [redacted]

39. [redacted]

40. [redacted]

[50] Paragraph 71, *In the Matter of Wireless E911 Location Accuracy Requirements*, FCC 15-9, PS Docket No. 07-114. January 29, 2015.

[redacted] [END CONFIDENTIAL]

41. Therefore, I conclude that T-Mobile's policy governing the use of customer location information is not sufficient to ensure customer data are protected against unauthorized use. These same risks could also leave Sprint customers unprotected if the companies are allowed to merge.

C. CONCLUSION

42. If this merger is approved, the confidential and personal information of millions of Sprint customers will be immediately available to T-Mobile's third-party suppliers. To ensure the merger would be in the public interest when it comes to customer data privacy and security, T-Mobile must clearly show that Sprint's customers' data will be secure when it is under T-Mobile's control. Not only has T-Mobile failed to demonstrate this over the course of this proceeding, the evidence suggests that T-Mobile's TPRM program contains gaps that could already be putting T-Mobile's customers at risk. Existing T-Mobile customers have already experienced significant privacy breaches that originated from T-Mobile's third-party suppliers. Since T-Mobile has failed to demonstrate their customer privacy protections are sufficient to protect consumers, and considering all of the evidence provided by the Pubic Advocates Office over the course of this proceeding, the Commission should deny the merger.

Attachment 1: Statement of Qualifications

Statement of Qualifications of Kristina Donnelly

1. My name is Kristina Donnelly. My business address is 505 Van Ness Avenue, San Francisco, California, 94102. I am a Public Utility Regulatory Analyst I with the California Public Utilities Commission ("CPUC") in the Communications and Water Policy Branch of the Public Advocates Office. I received a Bachelor of Science Degree in Mathematics from American University in Washington, D.C. in 2005 and a Master of Science degree in Natural Resources and Environmental Management from the University of Michigan in Ann Arbor in 2008.

2. I joined the Public Advocates Office in March 2018, where I work to advance the organization's mission and advocate on behalf of public utility customers. In my time with the Public Advocates Office, I have performed extensive research and analysis on a wide array of communications issues to inform the Public Advocates Office's decision-making and policy positions. I have also authored and/or contributed analysis to numerous Public Advocates Office comments, reports and filings on communications issues related to customer privacy (P. 18-03-014), affordability of utility services (R. 18-07-006), and the California Advanced Services Fund (CASF) (R. 12-10-012). Prior to my time with the Public Advocates Office, I was a Research Associate with the Pacific Institute, a non-profit organization, where I conducted water and energy policy research and analysis.

Attachment 2: TISS-610: Enterprise Third-Party (Supplier) Information Security Standard, T-Mobile Supplemental Response to Public Advocates Office DR 004, Attachment Titled "TMUS-CPUC-PA-00005629.Public_Enterprise Third-Party Information.pdf"

Enterprise Third-Party (Supplier) Information Security Standard

Approved by: Cyber Security & Privacy Policy Approver

1 Here's The Deal

The purpose of this TISS-610 Enterprise Third-Party (Supplier) Information Security Standard ("Standard") is to define T-Mobile's third-party information security requirements that help meet T-Mobile's overall risk management and security objectives.

Note – This Standard is aligned to the Enterprise Third-Party (Supplier) Risk Management Program. T-Mobile will complete an Enterprise (Supplier) Risk Management Program (ESRAP) intake for all Suppliers. The Cyber Assessment is triggered based off the results of the ESRAP intake.

2 What's In-scope

This Standard applies to all T-Mobile Third-Parties (suppliers) and T-Mobile personnel responsible for managing the supplier(s). This standard defines the security requirements that must be evaluated upon collaborating, changes in-scope-of-work and changes in the vendor security environment.

Third-Parties (Suppliers) includes, but not limited to, those performing any of the following:

1. Accessing, hosting, retaining, processing, or transmitting non-public T-Mobile information.
2. Developing, supporting, or managing technology, application(s), service(s), or solution(s) used for T-Mobile business purposes whether residing within T-Mobile's environment or hosted externally.
3. Any other work or partnership that, in T-Mobile's view, triggers a need to review or compare a party's processes, procedures, and policies.

3 Roles & Responsibilities

3.1 Supplier

Supplier is responsible for completing cyber assessment questionnaire and adhering the security requirements in this Standard to implement appropriate technological, procedural, and physical requirements controls to protect T-Mobile customers.

3.2 T-Mobile's Supplier Cyber Risk Management (SCRM) team

SCRM partners with T-Mobile's Enterprise (Supplier) Risk Management Program (ESRAP) to ensure T-Mobile meets certain compliance and regulatory obligations to protect T-Mobile customers and information, as defined in the Scope. As part of T-Mobile's broader Digital Security Organization (DSO), SCRM performs detailed Cyber Assessments to ensure suppliers are compliant with the Standard.

4 T-Mobile Third-Party (Supplier) Information Security Requirements

4.1 Information Handling Requirements

All T-Mobile information must be classified when created/received regardless of where it resides, the form it takes, or the technology used to handle it to enforce appropriate handling procedures as indicated in this Standard.

4.1.1 Information Classification

T-Mobile has defined an information classification scheme to properly identify all T-Mobile information. The information classification levels are used throughout this Standard. T-Mobile will determine the classification of the information you will be accessing, processing, and/or storing. Suppliers with multiple engagements at T-Mobile, must adhere to the requirements of the highest classification level they will be accessing, processing, and/or storing.

4.1.2 Information Handling for Customer Facing Applications, Systems and Activities

1. Customer-facing applications, systems, and/or activities that utilize Customer Proprietary Network Information (CPNI) must meet CPNI compliance requirements as defined in T-Mobile's CPNI requirements including practices for authentication of customers, notice of account changes, and unauthorized access incident tracking.
2. All systems/applications must be able to collect, track, and honor user preferences with respect to data collection including, but not limited to:
    a. Display a prominent notice and obtain affirmative consent of the user when collecting sensitive information about them;
    b. Capability to obtain and track consent and include links to a detailed notice, or
    c. Provide the option of opting out of data collection.
3. CPNI information must be stored within the boundaries of the United States.

4.1.3 Disposal of information Assets

All non-public T-Mobile information must be returned to T-Mobile or destroyed as defined in the contractual agreement. When Suppliers are performing media sanitation they must provide T-Mobile a certificate of destruction upon request. Please reach out to SCRM@T-Mobile.com for the form.

When destruction is carried out by a disposal vendor, it is essential the information is protected continuously from the time at which the information asset is sent for destruction, until the time the disposal vendor has picked up the data.

The following destruction methods must be used where applicable (unless other methods are described in the contractual agreement):

Information Assets	Disposal Method
Paper	Cross-cut shredding, incinerating, or pulping such that there is reasonable assurance the materials cannot be reconstructed.
Mobile Computing Devices (cell phones, tablets, etc.)	Delete all non-public T-Mobile information on the device(s).
Electronic Storage Media (hard drives, USB/memory sticks, RAM, tapes, etc.)	Physically destroy or sanitize media in accordance to NIST-800-88 Guidelines for Media Sanitization and verify removal of data.
Optical Disks (CDs, DVDs, etc.)	Use optical disk shredder or disintegrator. Disks can also be incinerated or grinders can be used.

4.2 *Incident Reporting*

Supplier must have the capacity to immediately notify T-Mobile of any security breach and must assist T-Mobile in investigating the security breach in accordance with terms of an approved contract, work order, or master service agreement. Supplier must have technical, administrative and physical security measures in-place so that vulnerabilities are disclosed responsibly, and that information about a security breach impacting T-Mobile information is not disclosed to the public until authorized to do so by T-Mobile.

4.3 *Encryption Requirements*

Encryption technologies must be used to protect T-Mobile Confidential and/or Restricted information. T-Mobile Confidential and/or Restricted data must be encrypted at rest and in-transit (over public data networks and/or within the Supplier's internal network).

1. Information Transmission: SSHv2, TLS1.2 or higher.
2. Encryption Standard: AES, RSA
    a. At Rest:
        i. Symmetric: AES 256 or higher
        ii. Asymmetric: RSAES-OAEP
    b. In-Transit:
        i. HTTPS, SSH, SFTP, Direct connection (dedicated circuit only for your scope of work with T-Mobile).
3. Usage of Proprietary Encryption Algorithm(s): must be reviewed, tested, and approved by T-Mobile.
4. Hashing Algorithm/Password Storage: SHA 2, Bcrypt, Scrypt, Other (upon approval of T-Mobile)
5. Wireless Networks: WPA2 (WPA1 and WEP must not be used)
6. MD5 and less must not be used

7. Unique T-Mobile encryption keys should be used for encryption of T-Mobile Confidential and/or Restricted information, where possible.
8. Salts must be random per user and a minimum of 16 characters in length.
9. User credentials must be encrypted during the authentication process when transmitted using a secure communications channel.
10. Passwords/authentication data must be hashed at rest any time the password is stored. Passwords must not be stored or transmitted in clear text (human readable form).

4.3.1 CRYPTOGRAPHIC REQUIREMENTS

Supplier must have clearly defined and documented processes for managing cryptographic keys.

1. Keys must be physically protected.
2. Keys must never be stored in locations that do not meet secure key management requirements.
3. Keys must be changed annually. Old keys must be retired or destroyed.
4. For high security keys, dual control or MFA must be implemented.
5. Key access must be restricted on a need to know basis.
6. Keys must be changed when employees with key access change job duties or leave the company.
7. Supplier using T-Mobile DNS domains must get their SSL/TLS certificates from T-Mobile.
8. All certificates used for T-Mobile purposes must have minimum key lengths of at least 2048 bits (RSA).
9. Passwords used to protect cryptographic keys must be as strong as the keys they protect.

4.4 ANTI-MALWARE

1. All systems supporting T-Mobile (e.g., external/internal servers, mobile computing systems, firewalls, web application firewalls, routers, and end User equipment) must be installed with current anti-malware software appropriate for their operating system, if applicable anti-malware technology exists.
2. Quick response procedures must be formally documented to detail actions in the event of a malware attack.
3. All anti-malware software must be actively running, updated with current definitions, and capable of generating logs. Centralized alerting must be enabled and monitored as part of the anti-malware solution.
4. End Users must not disable, bypass, or interfere with the anti-malware software security.

4.5 FACILITIES – PHYSICAL SECURITY

Physical security controls must be in-place to protect T-Mobile non-public information from unauthorized physical access, theft, and/or damage. The following controls are related to physical locations providing services to T-Mobile, including but not limited to: data centers, call centers, collection agencies, financial services, single tenant offices, multi-tenant offices, invoice processing, etc.

1. T-Mobile non-public information must be physically secured when not in use, including but not limited to, papers, manuals, and electronic media.
2. All areas of the premises storing and/or processing T-Mobile non-public information must be housed in secure areas and protected by a defined perimeter with appropriate security barriers and entry controls.
3. Facilities must be protected by intrusion alarms.
4. Alarms must be monitored twenty-four (24) hours per day, three hundred sixty-five (365) days per year.
5. Data centers must be equipped with dry fire suppression equipment or appropriate fire suppression equipment to prevent water damage to equipment supporting T-Mobile.
6. Access must be restricted to authorized personnel only.
7. Visitors must be required to present government issued photo identification prior to receiving access. Visitors awarded access to non-public areas must be escorted at all times in any area supporting T-Mobile.
8. Visitor logs must be maintained to provide an auditable trail of visitor activity. Visitor logs must be readily available for one year.
9. Visitor badges must expire automatically at the end of the work day.
10. Access rights to facilities must be based on business need and regularly reviewed and updated.
11. Access rights to facilities must be removed immediately upon notification of separation or a change in job responsibilities that no longer require physical access to the facility.
12. CCTV or other surveillance devices must be used to monitor individual physical access to sensitive areas and exterior entries where appropriate. The collected information must be reviewed and correlated with other entries. This data must be stored for a minimum of thirty (30) days for areas storing, processing, or transmitting T-Mobile non-public Information.
13. Physical access controls must exist for all network devices (e.g., wireless access points, gateways, and routers), data centers, telecommunications network facilities, and ancillary areas (e.g., generator, or UPS storage rooms); to ensure appropriate access by authorized individuals only.

4.6 Change Management

Suppliers must have documented change management processes. Changes to all systems and applications supporting T-Mobile must be properly approved, developed, tested, and implemented in a controlled and consistent manner to provide a level of confidentiality, availability, and integrity consistent with the importance of the services provided.

1. Changes on all network devices, applications, systems or databases include:
    a. Application changes – code or configuration
    b. Application patches
    c. System updates or patches
    d. Hardware changes
    e. Emergency changes
    f. Production data changes
2. Documented change control process must exist to include:
    a. Technical documentation and relevant user manuals must be updated.
    b. Documented evidence of approvals and testing.
    c. Testing plans and results must be documented and retained.
    d. Back-out plans must be documented prior to implementation.
    e. Emergency change procedures must be documented to include an established emergency approval authority.

4.7 Network Security

Appropriate network security controls must exist in Supplier's environment to ensure the confidentiality, integrity, and availability of the network, network devices, and information which support T-Mobile. If any of the following areas are not technologically possible, Supplier must notify SCRM@T-Mobile.com for determination of acceptable mitigation.

1. Appropriate network security controls must exist within Supplier's network to protect the network segment dealing with T-Mobile non-public information. The capability of Users to connect to and transmit/share T-Mobile non-public information between shared and segregated networks must be restricted on a least-privilege basis.
2. Network must have routing controls enabled to ensure access control requirements are met and the network is protected from breaches or attacks.
3. All access control lists and firewall rule sets related to systems supporting T-Mobile must be reviewed and approved by Supplier's management at least every 6 months.

4.8 Data Access Management

1. The Supplier is responsible and accountable for managing assets containing T-Mobile non-public information that are under the Supplier's control, and responsible for security controls relevant to any Supplier access to such assets.
2. Supplier with access to T-Mobile Confidential and/or Restricted information must have annual security and privacy awareness training programs based on the relevant role and responsibilities within the organization.

3. In a multi-tenant environment, there must be the ability to logically or physically segment data such that data may be accessed for a single tenant only, without inadvertently accessing another tenant's data (e.g., using unique identifiers or different schemas for each tenant.
4. If data will be stored, accessed, processed, and/or retained outside of the United States of America, the Supplier must contact ESRAP@T-Mobile.com for review and approval.
5. Back-up data containing non-public T-Mobile information must be segregated (physically or by using unique identifiers) from Supplier's information and Supplier's client's/customer's information with appropriate access controls to prevent unauthorized access.
6. If mobile devices will be utilized to transmit, receive, or store T-Mobile non-public information, a mobile device management solution must be used with the capability to remotely lock and wipe lost/stolen devices and to enforce disposal of information.

4.8.1 Logical Access Controls

1. Access right to systems accessing, processing, and/or storing T-Mobile non-public information must be granted on a least privilege basis. Access rights must be reviewed at least every 90 days. Inactive User accounts with no activity for more than 90 days must be removed and/or disabled.
2. Remote access to T-Mobile's environment(s) must be approved by a management-level single point of contact of the Supplier that will be responsible for enforcing T-Mobile security requirements.
3. MFA must be implemented for all remote elevated (privileged) network access for systems supporting T-Mobile.
4. User IDs must be unique and assigned to specific individuals.
5. User access rights to systems or information supporting T-Mobile must be deactivated within 72 hours upon Supplier's employee/contractor voluntary termination or change in job duties no longer requiring access. In the event of an involuntary termination, access must be removed immediately.
6. Creation of local admin groups and/or file shares must be added based on minimum necessary permissions and role-based appropriateness.

4.8.2 Password Complexity

1. Passwords (including default passwords) must be changed upon installment of the system or application, prior to launch in a production environment.
2. Group, shared, or generic accounts and passwords must not be used. Accounts must have an identified owner.
3. Passwords must not be displayed in clear text when being entered.
4. Systems must maintain a record of previous passwords and prevent re-use of at least the last 5 previously-used passwords.
5. Systems must lock accounts (User, Admin/Privileged, Service) after 30 minutes of idle activity or after 5 consecutive invalid login attempts.

The following are requirements for Account Types supporting or accessing T-Mobile environments.

Account Type	Requirements
User	1. Passwords must contain a minimum of 8 characters, and require: a mix of upper and lower case characters, include at least 1 number, and include at least one special character. 2. First time passwords must be a unique value and system must force password change on first use. *Note: If User chooses first password value, system does not need to force password change on first use.* 3. Password changes must be forced at least every 90 days.
Admin/ Privileged	1. Passwords must contain a minimum of 15 characters or, if not technically feasible, the system maximum. Passwords must meet the same complexity requirements as User accounts. 2. Admin/Privileged accounts must be separate from User accounts. 3. Passwords must be changed for all systems and user administrative accounts user had access to when user leaves organization or changes roles. 4. Password changes must be forced at least every 90 days.
Service (aka system passwords)	1. Passwords must contain a minimum of 30 characters (60 is preferred), and must meet same complexity requirements as User accounts. A password generation tool should be used to generate randomized passwords. 2. Must not be given interactive root or local administrator rights. 3. Passwords must be changed at least annually, or earlier in the case of security issues. 4. Passwords must not be shared beyond those with a demonstrated need to know. 5. Systems must not be able to select and change its own service account passwords. 6. Passwords must be immediately changed when a person with knowledge leaves the organization or changes roles. 7. Passwords must not be placed in ticket tracking systems.

	8. Must only be used for their approved service and not shared with systems/applications for which they were not provisioned.

4.8.3 Segregation of Duties

Segregation of duties (aka separation of duties) refers to dividing roles and responsibilities so that a single person cannot subvert a critical process.

1. Software developers must not have access to write/update/migrate code or changes to code in production systems.
2. Users must not be responsible for auditing the systems they are also responsible for maintaining.
3. While implementing segregation of duties, the principles of least privilege and need-to-know must be implemented.

4.9 Secure System and Software Development

Note: This section applies to systems or applications specifically developed or customized for T-Mobile. It may not apply to commercial off-the-shelf software without any customization.

1. Software applications must be developed based on industry best practices and include security through the software development life cycle (SDLC). T-Mobile may request documentation on Supplier's SDLC process. SDLC must use the following minimum guidelines:
    a. Defined duties based on job responsibility.
    b. Separate development, test, and production environments.
    c. Application code must be limited to appropriate personnel.
    d. Test data, vendor default accounts, tests accounts and passwords must be removed before production systems become active or are released to customers.
    e. Production data must not be used for development and testing.
    f. Secure code review checklist followed to ensure the following elements are addressed: structure, documentation, inputs, invalid characters, variables, arithmetic operations, loops and branches, defensive programming, error handling, access control, authentication and session management, efficiency, and support.
2. Applications must have strong authentication mechanisms, including user of minimum passwords or PIN lengths, lockout enforcement after 5 consecutive invalid login attempts, and logging and monitoring of failed login attempts.
3. Custom code must be peer reviewed, documented, and tested for security vulnerabilities. T-Mobile may request the documentation related to such reviews and testing.
4. Applications with non-public T-Mobile information must be developed taking into consideration the sensitivity of the information being handled.

a. Information must be masked during display in systems/applications where applicable (e.g., Social Security Numbers, bank account numbers, payment card information, passwords)
b. Cookies created for T-Mobile purposes may not be linked or linkable to an identifiable individual and must be encrypted and configured correctly. Sharing of cookies with third-parties must be as per the T-Mobile Privacy Policy.

5. For customer facing applications, customer (or potential customers) must have the ability to create their authentication credentials, except for temporary credentials

4.10 Vulnerability & Patch Management

Supplier must have documented, auditable vulnerability and patch management processes in-place for networks, hosts, and applications supporting T-Mobile. Processes must include, but are not limited to:

1. Vulnerability scans must be performed at least every ninety (90) days for the following:
   a. Authenticated scans and un-authenticated scans must be performed for internal/external web applications, hosts, network and web applications.
   b. Un-authenticated scans must be performed for external host and network scans.
2. Authenticated vulnerability scans must be performed for new systems/applications and/or enhancements to existing systems/applications prior to production deployment.
3. Supplier must retain vulnerability scan results supporting T-Mobile systems/applications for at least twelve (12) months from the date of the scan. Supplier must provide T-Mobile a copy of the most recent technical vulnerability assessment for systems supporting T-Mobile.
4. Supplier must ensure systems and applications are not operated past their End of Support lifecycle. All operating systems and applications must be on current, vendor supported versions (i.e., versions that still receive patches and updates) and Supplier must subscribe to vendor notifications of security threats and patches for each system/application supporting T-Mobile.
5. T-Mobile must be informed of vulnerabilities that may materially impact security as it relates to T-Mobile systems and data.
   a. High vulnerabilities (e.g., CVSS Base score of 7.0 or higher) must be remediated within thirty (30) days of vendor release/notification.
   b. Medium vulnerabilities (e.g., CVSS 6.9 to 4.0) - must be remediated within ninety (90) days of vendor release/notification.
   c. Lower risk vulnerabilities (e.g., CVSS below 4.0) - must be remediated within one hundred eighty (180) days or as requested by T-Mobile.
6. Suppliers must develop, maintain, and test security baseline configurations (hardened configuration) for platforms/systems supporting T-Mobile based on industry-accepted standards (i.e., CIS/SANS, ISO, NIST).

4.11 AUDITING & LOGGING

All network and information systems used for T-Mobile, in conjunction with the terms of contractual agreements, must be auditable and include the following requirements:

1. T-Mobile Confidential and/or Restricted data must not be contained in log files.
2. Procedures must ensure system activities are monitored for authorized use, access, and logging.
3. Level of auditing & logging must take into consideration the criticality of the application/process/system, the value, sensitivity and criticality of the information involved, system interconnection, past audit results, misuse, and system infiltration.
4. Auditing and logging must cover events including, but not limited to: authorized access, privileged operations, service accounts, unauthorized access attempts, systems alerts or failures, initialization of the audit logs, changes to or attempts to change system security settings and controls, errors and faults.
5. All events in the logs must be time-stamped. System times (clocks) must be synchronized via NTP (Network Time Protocol) to ensure accuracy of logs.
6. Log file retention for systems, applications, and/or databases supporting T-Mobile information:
   a. Must be stored to log server(s) or media that is difficult to alter;
   b. Must be stored for a minimum of 6 months.

4.12 SERVICE PARTNER CALL CENTERS

This section applies to Suppliers performing Call Center activities on behalf of T-Mobile related to existing or prospective T-Mobile customers. For Call Center physical security requirements refer to section 4.5.

1. The following is only allowed on production floors if pre-approved by T-Mobile in writing:
   a. Paper and the ability to print T-Mobile information.
   b. Usage of devices that may record audio, video and images. Any use of such equipment must comply with applicable law, and must be stored with security safeguards and access controls to limit access on a least-privilege basis.
   c. Access to the Internet
   d. Usage of Instant Messaging applications by agents with access to T-Mobile Confidential and/or Restricted information.
2. Computers supporting T-Mobile may only electronically connect to approved communication and support systems.
3. Call Centers handling T-Mobile's CPNI must have T-Mobile's annual security and privacy awareness training for workers with access to CPNI. Training sessions must be conducted, and materials distributed to personnel prior to commencement of services for T-Mobile. T-Mobile will determine if CPNI is in-scope.

4.13 External Audits

1. T-Mobile may request evidence of external audits and certifications.
2. Suppliers in scope for Sarbanes Oxley (SOX) and/or financial services must provide SSAE 16 or 18 SOC 1, Type 2 report upon request.
3. All suppliers in-scope for T-Mobile's PCI program must provide proof of PCI compliance, including but not limited to, their most recent (within the last 12 months) Attestation of Compliance for the scope of services supporting T-Mobile, for e.g., locations, payment applications, third-party service providers. T-Mobile reserves the right to request additional information/documentation, for e.g., Report on Compliance, Self-Assessment Questionnaire, compensating control worksheet, as needed. Supplier will document which PCI requirements they manage on behalf of or in coordination with T-Mobile.

5 Questions? - Get Help

- Contact SCRM@T-Mobile.com with any questions.

6 Exceptions

All cases of non-adherence to a T-Mobile Information Security policy, standard or procedure must be reported to SCRM@T-Mobile.com for evaluation. All material Supplier risks associated with T-Mobile customers, systems, and data must be treated and disclosed to T-Mobile (SCRM@T-Mobile.com).

7 More Info

1. T-Mobile Privacy Policy
2. Supplier Code of Conduct
3. T-Mobile CPNI Information

Attachment 3: TRS-610: Enterprise Third-Party (Supplier) Risk Management Standard, T-Mobile Supplemental Response to Public Advocates Office DR 004, Attachment Titled "TMUS-CPUC-PA-13000088(PUBLIC).pdf"

T · ·Mobile·

Version 1.0

TRS-610 ENTERPRISE THIRD-PARTY (SUPPLIER) RISK MANAGEMENT STANDARD

Approved by VP Internal Audit & Risk Management 2/29/2016

1 PURPOSE

The purpose of this Standard is to define T-Mobile third party risk management and security requirements that help meet T-Mobile's overall risk management objectives.

Note – this Standard was formerly known as TISS-610 Supplier Security Standard and is now aligned to the Enterprise Third-Party (Supplier) Risk Management program.

2 SCOPE

This Standard sets forth T-Mobile's requirements for Suppliers to take reasonable measures to implement appropriate technological and procedural controls to protect T-Mobile's information, business interests, and reputation.

This Standard applies to all Suppliers including, but not limited to, those performing any of the following:

1. Accessing, hosting, retaining, processing, or transmitting non-public T-Mobile information. Refer to the TISS-310 Information Classification Standard for descriptions of information classification levels.
2. Developing, supporting, or managing technology, application(s), service(s), or solution(s) used for T-Mobile business purposes whether residing within T-Mobile's environment or hosted externally.
3. Any other work or partnership that, in T-Mobile's view, triggers a need to review or compare a party's processes, procedures and policies.

2.1 DEFINITIONS

1. AOC – Attestation of Compliance (related to PCI).
2. CPNI – Customer Proprietary Network Information. CPNI is information related to T-Mobile Customer use of telecommunications services, such as: type of service or service plan, origination, destination or location of voice calls, and amount of use of telecommunication services. CPNI also includes information contained in customer bills. (CPNI is not subscriber list information – name, mobile phone number [MSISDN] and billing address.)
3. CVSS – Common Vulnerability Scoring System, an industry standard for assessing the severity of computer system security vulnerabilities. http://cve.mitre.org/cve/index.html
4. ESRA – Enterprise Third-Party (Supplier) Risk Assessment
5. ESRAP – Enterprise Third-Party (Supplier) Risk Assessment Program
6. FIPS/NIST – Federal Information Processing Standard (FIPS), a publicly announced standardization developed by the U.S. Federal Government for use in computer systems. NIST – National Institute of Standards and Technology, a measurement standards laboratory.
7. Must – Indicates requirements to be strictly followed in order to adhere to the policy (Standard) and from which deviation is prohibited unless a formal exception has been filed and granted.
8. Non-public T-Mobile information – this includes T-Mobile Restricted, Confidential and/or Internal information. Refer to TISS-310 Information Classification Standard (TISS-310) for examples and descriptions.
9. PCI – Payment Card Industry. Refer to TISS-310 for examples of PCI cardholder information.
10. PII – Personally Identifiable Information. Refer to TISS-310 for examples.
11. Public Data Network – a network established and operated by a telecommunications company, or a recognized private operating agency, for the specific purpose of providing data transmission services for the public. Data traversing a Public Data Network may be routed over numerous providers and via various means (e.g. wired and wireless). Based on routing protocols, network topologies, and network issues, the data may also be routed through a wide range of geographic locations including sent off-planet and returned via satellite.
12. RACI – Responsible, Accountable, Consulted and Informed.
13. ROC – Report on Compliance (related to PCI).

14. SAQ – Self Assessment Questionnaire (related to PCI).
15. Salt – In cryptography, a salt is random data that is used as an additional input to a one-way function that hashes a password or passphrase. Salts defend against dictionary attacks versus a list of password hashes, and against pre-computed rainbow table attacks.
16. Security breach – Actual, probable or reasonably suspected unauthorized access to, or acquisition, use, loss, destruction, compromise or disclosure of, any information maintained on the Supplier Systems.
17. Service accounts – Specially created accounts used to programmatically run a process or service on a server. A service account is often described as any account that does not correspond to an actual profile. Service accounts are usually used for connecting an application to a database, or machine-to-machine connectivity.
18. Should – Indicates the requirements to be followed in order to adhere to the policy (Standard) where possible. It indicates a preferred course of action that does not require a formal exception in case of the inability to meet a requirement.
19. SRMR – Supplier Risk Management Review (formerly known as SSA – Supplier Security Assessment, and ISVA – Information Security Vendor Assessment)
20. Third Party (a.k.a. Supplier/Vendor/Service Partner) – An external, third-party company, vendor, supplier, service provider or organization rendering services to or on behalf of T-Mobile.
21. T-Mobile Restricted and/or Confidential Information – as defined in TISS-310 Information Classification Standard (TISS-310).
22. User – Anyone who will have, or currently has, access to T-Mobile information and/or communication resources for the limited and express purpose of performing their job responsibilities.

3 ENTERPRISE THIRD-PARTY (SUPPLIER) RISK MANAGEMENT STANDARD

3.1 ENTERPRISE THIRD-PARTY (SUPPLIER) RISK ASSESSMENT PROGRAM - ESRAP

T-Mobile's Enterprise Third-Party (Supplier) Risk Assessment Program (ESRAP) was established to ensure that T-Mobile meets certain compliance and regulatory obligations to protect T-Mobile Information.

ESRAP includes, but is not limited to, the following domains: anti-corruption, financial health, financial services compliance, security and privacy, and related party transactions.

T-Mobile will complete an Enterprise Third Party (Supplier) Risk Assessment (ESRA) screening form for all Suppliers. All material Supplier risks associated with T-Mobile systems and data must be treated and disclosed to T-Mobile (ESRAP@t-mobile.com).

3.1.1 SUPPLIER RISK MANAGEMENT REVIEW - SRMR

ESRA is used as a trigger to determine if a SRMR is required. This Enterprise Third-Party (Supplier) Risk Management Standard (TRS-610) is the basis for the Supplier Risk Management Review (SRMR) which evaluates a Supplier's internal controls against the standards included in this document. To complete the SRMR, Suppliers provide a self-attestation via T-Mobile's Supplier Risk Management (SRM) questionnaire, third party independent audit reports (if available), and other supporting documents as requested. The SRMR is a desk review of those documents.

If the SRMR reveals a gap between the Supplier's internal controls and this Standard, a remediation plan and/or an exception request may be required.

All Suppliers in scope for T-Mobile's PCI compliance must provide proof of PCI compliance on request including, but not limited to, their most recent (within the last twelve (12) months) AOC. T-Mobile reserves the right to request additional information/documentation (e.g. ROC, SAQ, RACI) as needed.

Supplier will document which PCI requirements they manage on behalf of or in coordination with T-Mobile.

Note: The SRMR process does not apply to Suppliers that only provide contingent staffing using T-Mobile equipment. A SRMR is generally not required for Supplier's sub-contractors who simply support the Supplier's

work; however, this does not remove the obligation of the Supplier to ensure that T-Mobile's non-public information is secured appropriately as per this TRS-610, and as required by contractual terms between T-Mobile and Supplier.

3.1.2 THIRD PARTY CYBERSECURITY ASSESSMENT PROGRAM - CAP

T-Mobile's Corporate Information Security (CIS) Group, leads the Third Party Supplier (TPS) Cybersecurity Assessment Program (CAP) to perform detailed assessments and assurance of the Supplier Risk Management Review (SRMR).

The purpose of the Cybersecurity Assessment Program (CAP) is to identify whether appropriate security controls exist at T-Mobile's TPS in order to ensure the availability, integrity, and confidentiality of T-Mobile's data. This CAP review is focused on operational and technical security controls detailed in this TRS-610 Standard.

3.2 INFORMATION

T-Mobile has defined an information classification scheme to properly identify all T-Mobile information, TISS-310 Information Classification Standard (TISS-310). The information classification levels are used throughout this Standard. Please contact your T-Mobile representative if you need a copy of TISS-310.

Specific information handling procedures are identified in this Standard, TRS-610, to ensure that appropriate protection exists throughout the life cycle of the information based on T-Mobile's information classification level.

3.2.1 INFORMATION CLASSIFICATION

All T-Mobile information must be classified when created/received according to TISS-310 regardless of where it resides, the form it takes, or the technology used to handle it for the purpose of enforcing appropriate handling procedures as indicated in this Standard.

3.2.2 INFORMATION HANDLING, STORAGE, AND ASSETS

1. The Supplier is responsible and accountable for managing assets containing T-Mobile non-public information that are under Supplier's control, and responsible for security controls relevant to any Supplier access to such assets.
2. T-Mobile Restricted and/or Confidential Information must be physically secured when not in use, including but not limited to, papers, manuals, and electronic media.
3. Users should not store T-Mobile non-public information on personal devices/media.
4. T-Mobile Restricted and/or Confidential Information (data) must be encrypted while at rest.
5. In a multi-tenant environment there must be the ability to logically or physically segment data such that data may be accessed for a single tenant only, without inadvertently accessing another tenant's data (e.g. using unique identifiers or different schemas for each tenant).
6. T-Mobile must be advised if equipment or media containing non-public T-Mobile information is accessed, processed, or retained by Supplier's sub-contractor/service provider(s) or in any way has the ability to impact T-Mobile's security.
7. If data will be stored, accessed, processed, and/or retained outside of the United States of America, the Supplier must contact ESRAP@T-Mobile.com for review and approval.

3.2.3 BACK-UP INFORMATION HANDLING

1. Back-up data containing non-public T-Mobile information must be segregated (physically or by using unique identifiers) from Supplier's information or Supplier's client's/customer's information with appropriate access controls to prevent unauthorized access.
2. Back-up files should be stored in a remote location or secondary data center to reduce the risk of damage from a disaster at the main site. Back-up files for critical systems must be stored in a secondary location.
3. Back-up restoration procedures and media should be tested at least annually.

3.2.4 DISPOSAL OF INFORMATION

All non-public T-Mobile Information must be returned to T-Mobile or destroyed as defined in the contractual agreement. When Suppliers are performing media sanitation they must provide T-Mobile a certificate of destruction upon request. Please reach out to ESRAP@T-Mobile.com for the form.

The following destruction methods must be used where applicable (unless other methods are described in the contractual agreement):

Media	Disposal Method
Paper	Cross-cut shredding, incinerating, or pulping such that there is reasonable assurance the materials cannot be reconstructed.
Mobile Computing Devices (cell phones, tablets, etc.)	Delete all non-public T-Mobile information on the device(s).
Electronic Storage Media (hard drives, USB/memory sticks, RAM, tapes, etc.)	Physically destroy or sanitize media using a minimum of three overwrite passes and verify removal of data.
Optical Disks (CDs, DVDs, etc.)	Use optical disk shredder or disintegrator. Disks can also be incinerated or grinders can be used.

3.2.5 INFORMATION TRANSMISSION

1. T-Mobile Restricted and/or Confidential Information must be encrypted during transmission over public data networks.
2. When non-public T-Mobile information is being transmitted within the Supplier's internal network, encryption or appropriate network segmentation must be used (e.g. LAN/VLANs).

3.3 ENCRYPTION REQUIREMENTS

Encryption technologies must be used to protect T-Mobile Restricted and/or Confidential Information. When encryption is required, the following minimum technologies must be used:

1. Secure Shell (SSH)-2, Transport Layer Security (TLS)-1.2 for web based management and other remote access to systems containing or transmitting T-Mobile Restricted and/or Confidential Information.
2. Advanced Encryption Standard (AES), RSA, or other T-Mobile approved encryption algorithms must be used as the basis for encryption implementation.
    a. When using AES authenticated encryption, modes such as Counter with CBC-MAC (CCM) or Galois/Counter Mode (GCM) should be used when technically feasible.
    b. When using RSA, RSA Encryption Scheme - Optimal Asymmetric Encryption Padding (RSAES-OAEP) mode must be used.
3. In situations where there is an absolute need to use technologies that utilize proprietary encryption algorithms, these algorithms must be reviewed, tested, and approved by T-Mobile.
4. Encryption technologies must be used in accordance with government regulations of both the originating and destination countries. Please contact ESRAP@T-Mobile.com if the encryption technology does not meet T-Mobile's minimum requirements.
5. Proven standard hashing algorithms such as Secure Hash Algorithm (SHA)-2 (SHA-256 or above) must be used when cryptographic hashes are required (e.g. message integrity and digital signatures).
6. For password storage algorithms, the passwords must be hashed with SHA-2 or above and use a per-User account randomly generated salt. The passwords should be hashed with a stronger algorithm such as Password-Based Key Derivation Function 2 (PBKDF2), bcrypt or scrypt.
7. Salts must be random per-User and minimum of sixteen (16) characters in length. The same Salt can be used for security questions pertaining to a specific User.
8. MD5 message-digest algorithm (MD5) must **not** be used for encryption.

9. Unique T-Mobile specific encryption keys must be used for encrypting T-Mobile Restricted or Confidential Information where possible.
10. For wireless networks, Wi-Fi Protected Access (WPA2) should be used as a minimum basis of security. WPA1 and Wired Equivalent Privacy (WEP) must not be used.
11. The following minimum key lengths must be used for all encryption implementations:
    - 256 bits for hash algorithms
    - 128 bits for symmetric keys (256 bits recommended)
    - AES192 acceptable for IPsec tunneling (256 bits recommended)
    - 224 bits for Elliptic Curve (256 bits recommended)
    - 2048 bits for RSA Keys

3.3.1 CRYPTOGRAPHIC KEY MANAGEMENT

Suppliers must have clearly defined and documented processes for managing cryptographic keys (e.g. encryption, code signing, and/or authentication keys). It is recommended to use current FIPS/NIST standards as a basis.

Note: Cryptographic keys are considered T-Mobile Restricted and must be protected appropriately. Keys must be encrypted and never stored in clear text.

Cryptographic key management must include the following:

1. Equipment used to generate, store and archive keys must be physically protected.
2. Cryptographic keys must never be stored in equipment, documents or systems that are not provisioned to meet secure key management requirements (e.g. log files, ticket tracking systems, knowledge management systems, or training documentation).
3. Access to cryptographic keys must be restricted, limiting to the fewest number of custodians necessary.
4. Cryptographic keys must be changed (re-keyed) periodically:
    a. As deemed necessary and recommended by the associated application, preferably automatically.
    b. At least annually.
5. Old keys must be retired (archived, destroyed, or revoked as applicable).
    a. Encryption keys must be archived
    b. Signing keys must be destroyed
6. Key management procedures must be implemented for recovering keys that are lost, corrupted, or archived.
7. For high security keys, such as root certificate authority or trust anchor keys, key management procedures must be implemented to require split-knowledge and dual control of keys for operations such as export, rotation, or deletion. In some cases, dual control must also be implemented when the key is used for operations, for example using a Public Key Infrastructure (PKI) root Certificate Authority (CA) to sign a subordinate CA certificate. An example of dual control would be to require that two or three people each know only their own part of the key to reconstruct the whole key or the key must be divided and stored in two or more systems/devices.
8. Procedures must include a process for changing the keys in the event an employee with key management access (or knowledge) changes job duties or leaves the company.
9. Suppliers using T-Mobile DNS domains must get their SSL/TLS certificates from T-Mobile.
10. All the certificates used for T-Mobile purposes must have minimum key lengths of at least 2048 bits (RSA).
11. Passwords used to protect cryptographic keys must be as strong as the keys they protect.

    For example: A password must be twenty (20) characters long to protect a 128 bit AES symmetric key (or 2048 bit RSA key), where the password is randomly chosen from the printable ASCII characters (a-z, A-Z,

0–9, 32 special) characters. If the password for protecting cryptographic keys is User selected then it must be at least 112 characters long.

12. Virtual or web based key management involves the use of a service (using such methods as HTTPS or custom network protocols) that is used for the distribution of key material to servers/services. The key material includes such data such as private keys or account passwords, and extends to all forms of data used in authentication or data protection. If key management is virtual or web based, please contact ESRAP@T-Mobile.com for further review.

3.4 Disaster Recovery And Business Continuity

Supplier must implement and maintain a Disaster Recovery Plan that ensures all T-Mobile information that is identified to be the responsibility of the Supplier is backed-up and protected, is capable of being recovered, and that the integrity of all such recovered T-Mobile information is retained. This applies in the event that Supplier's network, application(s), interfaces, database(s), system(s) or facility(ies) experience a security breach or any significant interruption or impairment of operation, or any loss, deletion, corruption or alteration of data. Requirements for scope, recovery time, level of confidentiality, frequency of back-up, and security must be in accordance with the terms in an approved contract. For specific Business Continuity requirements based on tiering (e.g. Tier 1 requires full geographically dispersed Active-Active redundancy) please contact ESRAP@T-Mobile.com.

Back-up plans for individual systems should be tested at least annually to ensure that they meet the requirements of the Business Continuity Plan. For critical systems, back-up plans must cover all in-scope systems, information, applications, security, and data necessary to recover the complete system that is within Supplier's control in the event of a disaster. Documentation that a recovery plan is in place must be provided to T-Mobile upon request.

3.5 System Auditing, Logging And Monitoring

All network and information systems used for T-Mobile services, in conjunction with the terms of contractual agreements, must be auditable and include the following requirements:

1. T-Mobile Restricted and/or Confidential Information must be protected as per the security requirements in Section 3.2.1 and not be contained in log files with the exception of supporting temporary debugging processes. *Log files containing T-Mobile Restricted and/or Confidential Information must be deleted from all logging systems immediately upon bug resolution.*
2. Procedures must ensure system activities are monitored for authorized use, access, and logging.
3. The level of auditing and logging must take into consideration the criticality of the application/process/ system, the value, sensitivity and criticality of the information involved, the system interconnection, past audit results, misuse, and system infiltration.
4. Auditing and Logging must cover events including but not limited to: authorized access, privileged operations, unauthorized access attempts, system alerts or failures, initialization of the audit logs, changes to or attempts to change system security settings and controls, and logging of errors and faults.
5. All the events in the audit logs must be time-stamped. System times (clocks) must be synchronized via NTP (Network Time Protocol) to ensure the accuracy of audit logs. Where feasible, the clocks should be standardized to UTC time.
6. Log files for systems, applications, or databases supporting T-Mobile non-public information must be reviewed for anomalies on a regular basis, at least monthly. More frequent log reviews may be required by T-Mobile, dependent on the sensitivity of the system/data. T-Mobile may request evidence that log reviews are being done.
7. Log file retention for systems, applications, and/or databases supporting T-Mobile information:
    a. must be stored to log server(s) or media that is difficult to alter;
    b. must be stored for a minimum of six (6) months (recommended twelve (12) months);
    c. must be backed up; and
    d. In the event of a security breach T-Mobile may request to review log files.

3.6 LOGICAL ACCESS CONTROL

1. Access rights to systems storing and/or processing T-Mobile non-public information must be granted on a need-to-know and least-privilege basis using controls such as role-based access and segregation of duties.
2. Remote access to T-Mobile's internal environment must be approved by a management-level single point of contact (of the Supplier) that will be responsible for enforcing T-Mobile's security requirements defined in this TRS-610. This access must be reviewed for renewal at least every ninety (90) days.
3. Multi-factor authentication must be implemented for all remote elevated (privileged) network access for systems supporting T-Mobile. *(Multi-factor authentication requires the use of authentication elements from two (2) or more categories of something one has, something one knows, and/or something one is. Some examples are: a Smart Card plus password; or a security (electronic or software-based) token plus a password; or biometrics plus a password. The combination of a User ID and password does not qualify as multi-factor authentication.)*
4. User IDs must be unique and assigned to a specific individual. Group/Shared/Generic accounts must not be used.
5. User access rights to systems or information supporting T-Mobile must be deactivated within seventy-two (72) hours upon employee/contractor voluntary termination, leave of absence, or change in job duties no longer requiring access. In the event of an involuntary termination, access must be removed immediately.
6. Creation of local admin groups and/or file shares must be added based on minimum necessary permissions and role based appropriateness.
7. User access to each system, application, or database supporting T-Mobile must be documented and reviewed every ninety (90) days, at a minimum. Inactive User accounts with no activity for more than ninety (90) days must be removed and/or disabled. *The review does not extend to T-Mobile Customers who may be Users accessing a public facing system or application.*

3.7 NETWORK SECURITY CONTROLS

Appropriate network security controls must exist in Supplier's environment to ensure the confidentiality, integrity, and availability of the network, network devices, and information which support T-Mobile. If any of the following areas are not technologically possible, Supplier must notify ESRAP@T-Mobile.com for determination of acceptable mitigation.

1. Appropriate network security controls (e.g. firewalls, IDS/IPS, WAF), must exist within Supplier's network to protect the network segment dealing with T-Mobile non-public information. The capability of Users to connect to, and transmit/share T-Mobile non-public information between shared and segregated networks must be restricted based on business requirements and/or least-privilege basis.
2. Networks must have routing controls enabled to ensure access control requirements are met and the network is protected from breaches or attacks.
3. All access control lists and firewall rule sets affecting access to systems supporting T-Mobile must be reviewed and approved by Supplier's management at least every six (6) months.
4. All remote access to T-Mobile networks must be through T-Mobile approved methods. Please contact ESRAP@T-Mobile.com to ensure appropriate connectivity.

3.8 PASSWORD COMPLEXITY

The following (3.8.1, 3.8.2 and 3.8.3) are requirements for systems supporting T-Mobile or systems accessing T-Mobile's environment.

3.8.1 SERVICE ACCOUNT PASSWORDS

For service accounts (a.k.a., system passwords) that are not limited to either connecting an application to a database, or providing machine-to-machine connectivity, the following requirements apply:

1. All service accounts must have an identified owner.
2. Service account passwords must:

a. contain a minimum of thirty (30) characters, sixty (60) characters are recommended;
b. require a mixture of both upper and lower case characters;
c. include at least one (1) number and;
d. include at least one (1) special character (where technically feasible).

3. A password generation tool should be used to create randomized service account passwords.
4. Systems must maintain a record of previous passwords, and prevent re-use of at least the last five (5) previously-used passwords.
5. Service account passwords must be changed at least annually, or earlier in case of security issues.
6. Service account passwords must not be shared beyond those with a demonstrated need to know.
7. Passwords that are improperly disclosed must be changed immediately upon discovery.
8. System must not be able to select and change its own service account passwords.
9. System must lock service account after five (5) invalid login attempts and the account owner or system administrator must be notified to unlock the account.
10. Service accounts must only be used for their approved service and not shared with systems or applications for which they were not provisioned.
11. Service account passwords must be immediately changed when a person with knowledge of the password leaves the organization or changes roles and no longer requires access.
12. Service account passwords must not be placed in ticket tracking systems.
13. Service accounts must not be allowed to log in to systems interactively (e.g. with a human at a keyboard, rather than systematically). If interactive logins are possible (e.g. Database administrators) then the passwords for such accounts must be changed every 90 days in line with the privileged/administrator account requirement (refer to Section 3.8.3 Admin Account/Privileged Accounts).
14. Service accounts must not be given interactive root or local administrator rights.
15. Service accounts must have the minimum access (least privilege) required to run properly.
16. Service accounts must not be used as a group, team, or universal administration account.
17. All default service account passwords must be changed upon installment of the system or application and prior to launch in a production environment.

3.8.2 USER ACCOUNT PASSWORDS

The following are requirements for User accounts on systems supporting T-Mobile or systems accessing T-Mobile's environment. (These requirements are not intended for T-Mobile Customers – see Section 3.15 Customer-Facing Applications, Systems and Activities.)

1. Systems must enforce strong User passwords to:
    a. contain a minimum of eight (8) characters;
    b. require a mixture of both upper and lower case characters;
    c. include at least one number, and;
    d. include at least one special character (where technically feasible).
2. Passwords must not be shared.
3. Systems must:
    a. Prevent re-use of the five (5) previously-used passwords.
    b. Reset first-time passwords to a unique value for each User and force password to be changed on first use.
    c. Lock screens and require Users to re-enter their password after no more than thirty (30) minutes of idle activity.

d. Prevent passwords from displaying in clear text when being entered.

e. Enforce password changes at least every ninety (90) days.

f. Allow Users to select and change their own passwords and include a confirmation procedure to allow for input errors.

g. Automatically disable portable identification credentials (e.g. smart cards, identity tokens, RSA keys) that require the provision of a password to operate after five (5) consecutive invalid attempts. Systems must require an authorized administrator to unlock or reset the password on the locked account after proper authentication of the User.

h. Lock a User account after five (5) consecutive invalid login attempts and reset the password on the locked account after proper authentication of the User or a thirty (30) minute lock-out period.

4. User credentials (e.g. User ID and password) must be hashed or encrypted during the authentication process when transmitted using a secure communications channel (refer to Section 3.3 for Encryption Requirements).
5. Passwords/authentication data must be hashed at rest any time the password is stored (e.g. written to a disk, file or database, and salting must be implemented where feasible).
6. All default passwords must be changed upon installment of the system or application, and prior to launch in a production environment.

3.8.3 ADMIN ACCOUNT/PRIVILEGED ACCOUNTS

1. Admin/Privileged account passwords must be a minimum of fifteen (15) alphanumeric characters long, where technically feasible; where not technically feasible the system maximum must be used. If an account (privileged or other) has been compromised or suspected of being compromised, the affected passwords on systems must be immediately changed.
2. Privileged accounts (e.g. administrators) must be separated from User accounts.
3. Passwords of Admin/Privileged accounts must not be shared.
4. When a Privileged account User leaves the organization or changes roles, passwords must be changed immediately for all systems and administrative accounts to which the User had access.
5. Lock the account after five (5) consecutive invalid login attempts and reset the password on the account after proper authentication of the User or a thirty (30) minute lock-out period.
6. Group, shared, or generic accounts and passwords must not be used for system administration activities.
7. Passwords must be changed at least every ninety (90) days.
8. All default passwords must be changed upon installment of the system or application, and prior to launch in a production environment.

3.9 MOBILE DEVICE SECURITY

This section applies to Users who transmit, receive, or store T-Mobile Restricted and/or Confidential Information (e.g. email, attachments to email) via mobile devices. Mobile devices include, but are not limited to, smart phones, tablets, or handheld computing devices.

1. Mobile devices should be set for a maximum timeout for the device/system to lock after fifteen (15) minutes of inactivity.
2. A data wipe (of T-Mobile Restricted and Confidential Information) must be performed:

   a. after ten (10) unsuccessful password or passphrase attempts;

   b. after device is reported lost/stolen;

   c. on decommissioned devices, and/or;

   d. upon termination of Supplier services.

3. Users must enable the password controls for a mobile device containing T-Mobile Restricted and/or Confidential Information. Passwords on devices must not be simple and must require at least a four (4) character password (e.g. cannot be "1234, 1111, 9999"). Where possible, use of complex passwords must take precedence over using PINs.
4. Users should change the handheld security password/passphrase at least every ninety (90) days.
5. Users should not have the ability to disable password protection on mobile devices.

   To enforce the above controls, it is recommended that Suppliers should use a Mobile Device Management solution.

3.10 PHYSICAL CONTROLS

Physical security controls must be in place to protect T-Mobile Restricted and/or Confidential Information from unauthorized physical access, theft, and/or damage. The following controls are related to physical locations providing back-end services to T-Mobile, including but not limited to: data centers, call centers, collection agencies, financial services, invoice processing, etc.

1. All areas of the premises storing and/or processing T-Mobile Restricted and/or Confidential Information must be housed in secure areas and protected by a defined perimeter with appropriate security barriers and entry controls.
2. Facilities must be protected by intrusion alarms.
3. Alarms must be monitored twenty-four (24) hours per day, three hundred sixty-five (365) days per year.
4. Data centers must be equipped with dry fire suppression equipment or appropriate fire suppression equipment to prevent water damage to equipment supporting T-Mobile.
5. Access must be restricted to authorized personnel only.
6. Visitors must be required to present government issued photo identification prior to receiving access. Visitors awarded access to non-public areas must be escorted in any area supporting T-Mobile.
7. Visitor logs must be maintained and retained for at least thirty (30) days for locations providing back-end services to T-Mobile.
8. Visitor badges should expire at the end of the work day.
9. Access rights to facilities must be reviewed at least every ninety (90) days and updated as needed.
10. Access rights to facilities must be removed within seventy-two (72) hours upon employee/contractor voluntary termination, leave of absence, or those no longer requiring access. In the event of an involuntary termination, access must be removed immediately.
11. CCTV or other surveillance devices must be used to monitor individual physical access to sensitive areas and exterior entries where appropriate. The collected information must be reviewed and correlated with other entries. This data must be stored for a minimum of thirty (30) days for areas storing, processing, or transmitting T-Mobile Restricted and/or Confidential Information.
12. Physical access controls must exist for all network devices (e.g. wireless access points, gateways, and routers), data centers, telecommunications network facilities, and ancillary areas (e.g. generator, or UPS storage rooms); to ensure appropriate access by authorized individuals only.

3.11 CHANGE MANAGEMENT

Ensure that changes to all systems and applications supporting T-Mobile are properly approved, developed, tested, and implemented in a controlled and consistent manner to provide a level of confidentiality, availability, and integrity consistent with the importance of the services provided.

1. Changes on all network devices, applications, systems, or databases include:
   a. Application changes – code or configuration
   b. Application patches
   c. System updates or patches
   d. Hardware changes

e. Emergency changes
f. Production data changes

2. Documented change control process must exist to include:

   a. Technical documentation and relevant user manuals must be updated.
   b. Documented evidence of approvals and testing.
   c. Testing plans and results must be documented and retained.
   d. Back-out plans must be documented prior to implementation.
   e. Emergency change procedures must be documented to include an established emergency approval authority.

3.12 VULNERABILITY AND PATCH MANAGEMENT

1. Supplier must have documented auditable vulnerability and patch management processes in place for networks, hosts, and applications supporting T-Mobile including, but not limited to:

   a. System inventory
   b. Grouping and prioritization of technology resources
   c. Use of IT inventory and scope of related duties
   d. Managing remediation of vulnerabilities, threats, etc.
   e. Prioritizing vulnerability remediation
   f. Maintaining an organization-specific remediation database
   g. Testing remediation prior to deployment
   h. Deployment of vulnerability remediation
   i. Distribution of vulnerability and remediation information to administrators
   j. Verifying remediation was effective

2. Authenticated vulnerability scans must be performed for new systems/applications and/or enhancements to existing systems/applications prior to production deployment. Supplier must retain vulnerability scan results supporting T-Mobile systems/applications for at least twelve (12) months from the date of the scan.

3. Upon request, Supplier must provide T-Mobile a copy of the most recent technical vulnerability assessment for systems supporting T-Mobile. As defined in the contractual agreement T-Mobile may also request scans or perform scans on the Suppliers environment and any application that is being developed on behalf of T-Mobile.

4. Vulnerability scans must be performed at least every ninety (90) days for the following:

   a. Authenticated scans and un-authenticated scans must be performed for internal/external web applications, hosts, network and web applications.
   b. Un-authenticated scans must be performed for external host and network scans.

5. Vulnerability scans must be performed after any significant change in the network, host ,application or system environment such as:

   a. New system component installations
   b. Changes in network topology
   c. Firewall rule modifications
   d. Application/hardware/software updates

6. Rescans must be performed to ensure the identified vulnerabilities are corrected.

7. Network intrusion and monitoring systems must immediately send notification to administrative personnel of unusual activity and suspected compromises.

8. T-Mobile must be informed of vulnerabilities that may materially impact security as it relates to T-Mobile systems and data.

   a. High vulnerabilities (e.g. CVSS Base score of 7.0 or higher) must be remediated within thirty (30) days of vendor release/notification.

   b. Medium vulnerabilities (e.g. CVSS 6.9 to 4.0) - must be remediated within ninety (90) days of vendor release/notification.

c. Lower risk vulnerabilities (e.g. CVSS below 4.0) - must be remediated within one hundred eighty (180) days or as requested by T-Mobile.

9. Supplier must ensure systems and applications are not operated past their End of Support lifecycle. All operating systems and applications must be on current, vendor supported versions (i.e. versions that still receive patches and updates).
10. Suppliers must subscribe to vendor notifications of security threats and patches for each technology platform/application supporting T-Mobile.
11. Secure Configuration Management - Suppliers must develop, maintain, and test security baseline configurations (hardened configuration) for platforms supporting T-Mobile based on industry-accepted system-hardening standards, which may include but are not limited to:

    a. Center for Internet Security (CIS)
    b. International Organization for Standardization (ISO)
    c. SysAdmin Audit Network Security Institute (SANS)
    d. National Institute of Standards Technology (NIST)

3.13 ANTI-MALWARE

1. All systems supporting T-Mobile (e.g. external/internal servers, mobile computing systems, firewalls, web application firewalls, routers, and end User equipment) must be installed with current anti-malware software appropriate for their operating system, if applicable anti-malware technology exists.
2. All anti-malware software must be actively running, updated with current definitions, and capable of generating logs. Centralized alerting must be enabled and monitored as part of the anti-malware solution.
3. End Users must not disable, bypass, or interfere with the anti-malware software security.
4. The anti-malware software must be enabled for periodic scans.
5. Alerts must be generated in the event that the anti-malware software is disabled on systems supporting T-Mobile (e.g. external/internal servers, database servers, file servers, firewalls, web application firewalls and routers).
6. Care should be taken to protect against the introduction of malicious code during maintenance and emergency procedures which may bypass normal malicious code protection controls.
7. Quick response procedures must be formally documented to detail actions in the event of a malware attack.

3.14 SECURE SYSTEM AND SOFTWARE DEVELOPMENT

This section applies to systems or applications specifically developed for T-Mobile. *It does not apply to commercial off-the-shelf software.*

1. To prevent errors, loss, unauthorized modification, or misuse of information in applications, appropriate controls must exist to ensure correct processing. These controls must include the validation of input data, internal processing, and output data.
2. Software applications must be developed based on industry best practices and include information security throughout the software development life cycle (SDLC). T-Mobile may request documentation on Supplier's SDLC process. SDLC must use the following minimum guidelines:

    a. Defined duties based on job responsibility (refer to Section 3.16 Segregation of Duties).
    b. Separate development, test, and production environments.
    c. Application code must be limited to appropriate personnel.
    d. Remove test data, vendor default accounts, test accounts and passwords before production systems become active or are released to customers.
    e. Where technically possible, use stored procedures rather than scripts.

3. Production data must NOT be used for development and testing.
4. Developers should have knowledge of secure coding techniques such as the OWASP Guidelines for web development (http://www.owasp.org) or other industry known best practices.

5. A code review checklist should be followed to ensure the following elements, at a minimum, are addressed: structure, documentation, inputs, invalid characters, variables, arithmetic operations, loops and branches, defensive programming, error handling, access control, authentication and session management, efficiency, and support.
6. Custom application code must be reviewed as per Section 3.11 Change Management - to identify vulnerabilities prior to production release.
7. Applications must include strong authentication mechanisms, including the use of minimum password or PIN lengths (refer to Section 3.8 Password Complexity), lockout enforcement after five (5) consecutive incorrect login attempts, and logging and monitoring of failed login attempts. Additionally, where applicable, brute force prevention techniques, such as CAPTCHA, must be utilized to help mitigate automated password guessing attacks.
8. Custom Code developed for systems or applications supporting T-Mobile must be peer-reviewed, documented, and tested for security vulnerabilities as applicable, including, but not limited to, the following:
    a. Injection flaws (e.g. SQL injection)
    b. Cross Site Scripting (XSS)
    c. Broken authentication/session management (e.g. use of account credentials and session cookies)
    d. Insecure Direct Object Reference
    e. Cross Site Request Forgery (CSRF)
    f. Security misconfiguration
    g. Insecure cryptographic storage
    h. Failure to restrict URL access
    i. Insecure communications
    j. Insufficient Transport Layer Protection
    k. Un-validated redirects and forwards
    l. Buffer overflows
    m. Improper error handling

    T-Mobile may request the documentation related to such reviews and testing.
9. Applications must disable output of specific detailed error messages to the client (end User equipment) and display only a common generic message.
10. Applications dealing with T-Mobile Restricted and/or Confidential Information must be developed taking into consideration the sensitivity of the information being handled.
    a. T-Mobile Restricted Information must be masked during display in systems/applications where applicable (e.g. Social Security Numbers, bank account numbers, payment card numbers, passwords).
    b. Cookies created for T-Mobile business purposes must not contain User PII data, and must be encrypted and configured correctly. Sharing of cookies with third-parties must be as per the T-Mobile Privacy Policy.

3.15 CUSTOMER-FACING APPLICATIONS, SYSTEMS AND ACTIVITIES

Requirements in this section are specific to systems or applications that are or will be accessed by existing or potential T-Mobile Customers:

1. Customer-facing applications, systems, and/or activities that utilize customer CPNI (Customer Proprietary Network Information) must meet CPNI compliance requirements as defined in T-Mobile's CPNI policy, including practices for authentication of customers, notice of account changes, and unauthorized access incident tracking (refer to Definitions – Section 2.1 for additional description). Please contact your T-Mobile representative to determine if CPNI is in scope and request the CPNI Policy (TISD-1039), if applicable.

2. All projects/systems must be able to collect, track, and honor user preferences with respect to data collection. Specific requirements will be provided in project requirements documents or statement of work, and could include:
    a. the capability to display a prominent notice and obtain affirmative consent of the User when collecting sensitive information about them;
    b. capability to obtain and track consent and include links to detailed notice, or
    c. the option of opting out of data collection.

    Requirements will be driven in part by principles stated in the T-Mobile Privacy Policy.
3. A unique randomly generated password should be used for initial value or reset password. The system should require a password change on first authentication.
4. Only the Customer (or potential Customers) must have the ability to create their authentication credentials, except for temporary credentials.
5. Customer account passwords must be complex with a minimum of eight (8) alpha-numeric characters.
6. Customer passwords, including secondary passwords and answers to security questions, must be hashed (as per Encryption Requirements - Section 3.3).

3.16 SEGREGATION OF DUTIES

Segregation of duties (a.k.a. Separation of duties) refers to dividing roles and responsibilities so that a single person cannot subvert a critical process.

1. Software developers must not have access to write/update code in production systems. They may have read only access to such systems to perform their job responsibilities.
2. Software developers must not have access to migrate changes into the production environment (the purpose is to have segregation of duties, so if, for example, code is developed by one developer on the team, another developer on the team can migrate the code to production).
3. In the event of an emergency break fix in production, logging of access and events must occur (e.g. firefighter process). Once they are done, the person must document what changes were made associated to the event.
4. Development, testing, and production environments must be properly separated. Functionality and operations should not overlap.
5. Supplier-developed applications must be reviewed for vulnerabilities by individuals other than the developers of the application.
6. At no time shall a person be responsible for auditing the systems that they are also responsible for maintaining.
7. While implementing segregation of duties, the principles of least-privilege and need-to-know must be implemented.

3.17 INCIDENT REPORTING

Supplier must have the capacity to immediately notify T-Mobile of any Security Breach and must assist T-Mobile in investigating the Security Breach in accordance with terms of an approved contract, work order, or master service agreement. Supplier must have technical, administrative and physical security measures in place so that vulnerabilities are disclosed responsibly, and that information about a Security Breach impacting T-Mobile information is not disclosed to the public until authorized to do so by T-Mobile.

3.18 CALL CENTERS

This section applies to Suppliers (Service Partners) performing Call Center activities on behalf of T-Mobile, related to existing or prospective T-Mobile Customers.

1. Call center production floor environments must be paperless and not allow for the printing of T-Mobile information, unless pre-approved in writing by T-Mobile.

2. Devices that may record audio, video and images (e.g. cameras, mobile devices) are not permitted on call center production floor environments, unless pre-approved in writing by T-Mobile. If Supplier uses audio, video, or image recording devices for call center security, use of such devices shall be in compliance with applicable law, and any recordings of call center activity must be stored with reasonable security safeguards and access controls to limit access to authorized investigative personnel.
3. Call center computers supporting T-Mobile must be configured to prevent Users/agents from storing T-Mobile non-public information to their computer or to removable media (e.g. tapes, disks, USB drives, removable external hard drives, CDs, DVDs).
4. Call center computers supporting T-Mobile may only electronically connect to approved communication and support systems. Access to the Internet is generally not permitted, though may be allowed subject to the call center passing certain security controls and in agreement with contractual terms acceptable to T-Mobile.
5. Instant Messaging applications must be pre-approved for use by T-Mobile in writing for those Users/agents who access T-Mobile Restricted and/or Confidential Information.
6. Call Centers handling T-Mobile's Customer Proprietary Network Information (CPNI) must have T-Mobile's annual security and privacy awareness training programs for workers with access to CPNI. Training sessions must be conducted and materials distributed to personnel prior to commencement of services for T-Mobile. Please contact your T-Mobile representative to determine if CPNI is in-scope and request assistance if needed.

3.19 SECURITY & PRIVACY AWARENESS

Suppliers with access to T-Mobile Restricted and/or Confidential Information must have annual security and privacy awareness training programs based on the relevant role and responsibilities within the organization.

3.20 EXCEPTIONS/INABILITY TO MEET STANDARDS

In the event the Supplier is unable to meet any of the requirements in this Standard TRS-610, please notify ESRAP@T-Mobile.com to discuss compensating controls or to determine if mitigation is required.

4 REFERENCES

1. TISS-310 Information Classification Standard
2. T-Mobile Privacy Policy
3. TISD-1039 Handling Customer Proprietary Network Information (CPNI)
4. TLS-210 Records Retention Schedule Standard

Attachment 4: Cyber Assessment Questionnaire, T-Mobile Supplemental Response to Public Advocates Office DR 004, Confidential Attachment Titled "TMUS-CPUC-PA-00005641.Confidential.xlsx"

CONFIDENTIAL

Attachment 5: Supplier Risk Management (SRM) Questionnaire, T-Mobile Supplemental Response to Public Advocates Office DR 004, Confidential Attachment Titled "TMUS-CPUC-PA-00005642.Confidential.xlsm"

CONFIDENTIAL

Attachment 6: "TLP-500 Customer Location Information Policy," T-Mobile Supplemental Response to Public Advocates Office DR 004, Confidential Attachment Titled "TMUS-CPUC-PA-00005626.Confidential_customer Location information policy.pdf"

CONFIDENTIAL

Attachment 7: T-Mobile Response to Public Advocates Office Data Request 007, Questions 7-10, 7-12, and 7-13

BEFORE THE PUBLIC UTILITIES COMMISSION

OF THE STATE OF CALIFORNIA

In the Matter of the Joint Application of Sprint Communications Company L.P. (U-5112-C) and T-Mobile USA, Inc., a Delaware Corporation for Approval of Transfer of Control of Sprint Communications Company L.P. Pursuant to California Public Utilities Code Section 854(a)	))))))	Application No. 18-07-011
In the Matter of the Joint Application of Sprint Spectrum L.P. (U-3062-C), and Virgin Mobile USA, L.P. (U-4327-C) and T-Mobile USA, Inc., a Delaware Corporation for Review of Wireless Transfer Notification per Commission Decision 95-10-032	))))))	Application No. 18-07-012

[PUBLIC VERSION]

T-MOBILE USA'S RESPONSE TO THE CALIFORNIA PUBLIC ADVOCATES OFFICE'S DATA REQUEST 007

Dave Conn
Michele Thomas
Susan Lipper
T-Mobile USA, Inc.
12920 SE 38th St.
Bellevue, WA 98006
Telephone: 425.378.4000
Facsimile: 425.378.4040
Email: dave.conn@t-mobile.com
michele.thomas@t-mobile.com
susan.lipper@t-mobile.com

Suzanne Toller
Davis, Wright, Tremaine LLP
505 Montgomery Street, Suite 800
San Francisco, CA 94111
Telephone: (415) 276-6536
Facsimile: (415) 276-6599
Email: suzannetoller@dwt.com

Leon M. Bloomfield
Law Offices of Leon M. Bloomfield
1901 Harrison St., Suite 1400
Oakland, CA 94612
Telephone: 510.625.1164
Email: lmb@wblaw.net

Attorneys for T-Mobile USA, Inc.

Dated: January 3, 2019

Data Request 7-10.

Who is responsible for conducting the SRMR?

Response to Data Request 7-10.

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to temporal scope and the phrases "conducting" and "SRMR." T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile's risk evaluation processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds that the TPRM Program has ultimate oversight and strategic responsibility for the supplier assessment processes, including the Cyber Assessment (formerly known as the SRMR); see Response to Cal PA DR 7-8 above.

Data Request 7-12.

After establishing a relationship with a supplier, does T-Mobile conduct subsequent or periodic screenings or reviews of supplier security practices and procedures?

Response to Data Request 7-12.

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to the phrases "establishing a relationship" and "supplier security practices and procedures." T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile's risk evaluation processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds that it periodically re-reviews suppliers throughout the course of the engagement on a cadence that depends on any issues or concerns that were identified in the initial review of the Cyber Assessment, and/or in response to intervening events such as a reported breach or other incident where the TPRM Program may determine that an additional review is necessary.

Data Request 7-13.

If so, are screenings or reviews conducted regularly or only when triggered? If screenings or reviews are conducted regularly, please indicate their frequency. If screenings or reviews are conducted only when triggered, please describe what conditions would trigger a review.

Response to Data Request 7-13.

T-Mobile objects to this Data Request on the grounds it is vague and ambiguous with respect to temporal scope and the phrases "screenings or review" and "triggered." T-Mobile further objects to this Data Request on the grounds it seeks information which is neither relevant to the pending Wireline or Wireless Applications nor reasonably calculated to lead to the discovery of relevant information as, among other things, T-Mobile's risk evaluation processes for new suppliers has no bearing on whether the transfer of Sprint Wireline is adverse to the public interest or to any appropriate review of the Sprint Wireless Transfer Notification.

Subject to and without waiving its objections, T-Mobile responds that new Cyber Assessments are performed regularly (e.g., on three-year, 18-month, 12-month or 6-month cycles) for all suppliers depending on their initial Cyber Assessment. New Cyber Assessments may also be required of a supplier in various circumstances including in response to a reported event, change in control, or for some other issue or concern that may come to T-Mobile's attention. See also Response to Cal PA DR 7-12 above.

Attachment 8: T-Mobile Supplemental Response to Public Advocates Office Data Request 010, Questions 10-8, 10-14, and 10-15

BEFORE THE PUBLIC UTILITIES COMMISSION

OF THE STATE OF CALIFORNIA

In the Matter of the Joint Application of Sprint Communications Company L.P. (U-5112-C) and T-Mobile USA, Inc., a Delaware Corporation for Approval of Transfer of Control of Sprint Communications Company L.P. Pursuant to California Public Utilities Code Section 854(a)	)))))))	Application No. 18-07-011
In the Matter of the Joint Application of Sprint Spectrum L.P. (U-3062-C), and Virgin Mobile USA, L.P. (U-4327-C) and T-Mobile USA, Inc., a Delaware Corporation for Review of Wireless Transfer Notification per Commission Decision 95-10-032	)))))))	Application No. 18-07-012

[PUBLIC VERSION]

T-MOBILE USA'S SUPPLEMENTAL RESPONSE TO THE CALIFORNIA PUBLIC ADVOCATES OFFICE'S DATA REQUEST 010

Dave Conn
Michele Thomas
Susan Lipper
T-Mobile USA, Inc.
12920 SE 38th St.
Bellevue, WA 98006
Telephone: 425.378.4000
Facsimile: 425.378.4040
Email: dave.conn@t-mobile.com
michele.thomas@t-mobile.com
susan.lipper@t-mobile.com

Suzanne Toller
Davis, Wright, Tremaine LLP
505 Montgomery Street, Suite 800
San Francisco, CA 94111
Telephone: (415) 276-6536
Facsimile: (415) 276-6599
Email: suzannetoller@dwt.com

Leon M. Bloomfield
Law Offices of Leon M. Bloomfield
1901 Harrison St., Suite 1400
Oakland, CA 94612
Telephone: 510.625.1164
Email: lmb@wblaw.net

Attorneys for T-Mobile USA, Inc.

Dated: April 5, 2019

Data Request 10-8.

On page 3, line 23 of Susan Brye's Rebuttal Testimony, Ms. Brye references "other assessments," besides the Cyber Assessment. Please provide a comprehensive list of all assessments T-Mobile conducts when evaluating the risks posed by third-party suppliers. For each assessment, please indicate:

a. Who is responsible for completing the assessment.
b. Who at T-Mobile is responsible for reviewing the assessment.
c. At what point in the relationship the assessment is completed.
d. Whether the assessment is mandatory for all suppliers or only a subset. If the assessment is only conducted for a subset of suppliers, please indicate the conditions that would trigger the assessment.
e. Whether the assessment is conducted once or periodically throughout the third-party relationship. If the assessment is conducted periodically, please indicate how frequently the assessment is conducted and what triggers a re-assessment.

Response to Data Request 10-8 (February 22, 2019).

See T-Mobile's Response to Cal PA DR 10-1 above.

Supplemental Response to Data Request 10-8.

Subject to and without waiving its objections, and pursuant to ALJ Bemesderfer's March 25, 2019 ruling granting Cal PA's Motion to Compel, T-Mobile responds

a. See T-Mobile Response to Cal PA DR 10-3 above.

b. TPRM analysts have primary responsibility for reviewing non-cyber assessments. Analysts on the Supplier Cyber Risk Management team within the Digital Security Office have primary responsibility for reviewing Cyber Assessments. TPRM's managers and/or the TPRM Senior Director may also review certain assessments, typically at the request of an analyst depending on the circumstances.

c. TPRM assessments are completed prior to engagement/re-engagement of a supplier. TPRM review is triggered when the internal T-Mobile business owner contacts Procurement to engage a supplier. As a general matter, the TPRM analyst sends the internal risk assessment to the internal T-Mobile business owner and the external assessments to the supplier within 2-business days of that notification to Procurement. TPRM's review must be complete prior to contract signature.

T-Mobile further responds that the TPRM Program is designed to adjust the scope of review based on the inherent risk of an engagement. TPRM assigns every supplier engagement a "service" and "sub-service category" based on the scope of

services that are then mapped to risk assessments TPRM requires for that engagement. See also TPRM Service-Category Assessment Mapping attached as confidential the document beginning with Bates No. TMUS-CPUC-PA-00005959. Depending on the circumstances, the TPRM analyst may add additional assessments to the mix prescribed if the supplier's scope of services indicate a higher level of inherent risk; i.e., the risk associated with the service provided, not the particular identity of the supplier engaged to perform those services (for example, an engagement that requires access to T-Mobile customer data has the highest possible inherent risk score). Conversely, the TPRM analyst may reduce the required assessments if the nature of the supplier's expected services do not require a particular assessment. For example, a business continuity assessment may be waived for a supplier engaged on a short-term basis. The decision process for adding or reducing assessments from what is prescribed is documented within TPRM and exceptions are reviewed to confirm consistency among analysts and to identity potential issues.

d. TPRM review is mandatory for all suppliers prior to engagement.

e. TPRM requires existing suppliers to periodically re-complete each risk assessment, which are reviewed and re-scored. The frequency depends on the supplier's last inherent risk scores (per assessment):

[BHC-AEO]

[redacted]

[EHC-AEO]

If an internal T-Mobile business unit seeks to re-engage a supplier before TPRM's scheduled re-review, TPRM will cancel the re-review and instead require a new set of risk assessments as part of the new engagement. The supplier's completion of a new set of risk assessments will reset the re-review clock within TPRM and the new frequency will be based on the new risk scores.

Data Request 10-14.

On page 7, line 16-19 of Susan Brye's Rebuttal Testimony, T-Mobile states that "suppliers are now required to undergo an even more comprehensive review, including a detailed Cyber Assessment…if certain conditions are present," and provided one example of one condition that would trigger an "even more comprehensive review."

a. Please describe all of the conditions that would trigger an "even more comprehensive review."

b. Please describe all of the steps that would be followed under the "even more comprehensive review," in addition to the detailed Cyber Assessment that T-Mobile already mentioned.

Response to Data Request 10-14 (February 22, 2019).

See T-Mobile's Response to Cal PA DR 10-1 above.

Supplemental Response to Data Request 10-14.

Subject to and without waiving its objections, and pursuant to ALJ Bemesderfer's March 25, 2019 ruling granting Cal PA's Motion to Compel, T-Mobile responds as follows:

a. Ms. Brye's testimony refers to the evolution of the TPRM Program, including replacement of the former Supplier Risk Management Review (a cyber assessment) with the new Cyber Assessment that went into effect in July 2018. The review under the TPRM Program as described in Ms. Brye's testimony is "even more comprehensive" because TPRM now assesses suppliers using a greater number (i.e., currently thirteen (13)) of unique risk domains than used under prior iterations of the program.

b. See T-Mobile's Responses to Cal PA DRs DR 10-3, 10-8, 10-9 and 10-14 above.

Data Request 10-15.

On page 7, lines 20-21 of Susan Brye's Rebuttal Testimony, T-Mobile states, "New TISS-610 better aligns with NIST standards, technology advancements, and security industry best practices."

a. Please provide a description of all of the specific changes that were made between the previous TRS-610 program and the new TISS-610, and how they better align the TPRM program with NIST standards, technology advancements, and security industry best practices.

b. Have T-Mobile's existing third-party relationships been subject to re-review under the new TPRM Program?

i. If so, when did T-Mobile complete these re-evaluations?

ii. If not, why not?

Response to Data Request 10-15 (February 22, 2019).

See T-Mobile's Response to Cal PA DR 10-1 above.

Supplemental Response to Data Request 10-15.

Subject to and without waiving its objections, and pursuant to ALJ Bemesderfer's March 25, 2019 ruling granting Cal PA's Motion to Compel, T-Mobile responds as follows:

a. The two policies are very similar in substance; however, new TISS-610 released to improve readability and present T-Mobile's supplier security requirements in a more accessible and understandable format (e.g., plain language in a T-Mobile "Uncarrier" format). Additionally, the security domains covered in that policy were reordered and are now presented in the same order as questions the supplier must complete under the new TPRM Cyber Assessment that went into effect in July 2018. Suppliers can now better track T-Mobile's cyber security requirements in line with the questions/information T-Mobile seeks in that assessment, thereby reducing questions and facilitating the supplier's clearer understanding of T-Mobile's requirements for access to non-public data.

b. Since June 2018, existing suppliers who have come up for re-engagement have come through the new TPRM Program. During the same time, the TPRM Program has been used to review existing suppliers who have come due for re-review assessments. See also T-Mobile's Response to Cal PA DR 10-8 above.

i. See T-Mobile's Response to Cal PA DR 10-8 above.

ii. See T-Mobile's Response to Cal PA DR 10-8 above.