



Independent Assessor's Report on Twitter, Inc.'s Information Security Program

For the period September 13, 2015 – September 12, 2017

The contents of this document, including the Report of Independent Accountants, contain PricewaterhouseCoopers LLP proprietary information that shall be protected from disclosure outside of the U.S. Government in accordance with the U.S. Trade Secrets Act and Exemption 4 of the U.S. Freedom of Information Act (FOIA). The document constitutes and reflects work performed or information obtained by PricewaterhouseCoopers LLP, in our capacity as independent assessor for Twitter, Inc. for the purpose of the Twitter, Inc. Order. The document contains proprietary information, trade secrets and confidential commercial information of our firm and Twitter, Inc. that is privileged and confidential, and we expressly reserve all rights with respect to disclosures to third parties. Accordingly, we request confidential treatment under the Freedom of Information Act (FOIA), the U.S. Trade Secrets Act or similar laws and regulations when requests are made for the report or information contained therein or any documents created by the FTC containing information derived from the report. We further request that written notice be given to PwC and Twitter, Inc. before distribution of the information in the report (or copies thereof) to others, including other governmental agencies, to afford our firm and Twitter, Inc. with the right to assert objections and defenses to the release of the information as permitted under FOIA or other similar applicable law or regulation, except when such distribution is already required by law or regulation. This report is intended solely for the information and use of the management of Twitter, Inc. and the U.S. Federal Trade Commission and is not intended to be and should not be used by anyone other than these specified parties.



Table of Contents

Introduction	3
Report of Independent Accountants	4
Twitter Information Security Program Overview	6
PwC's Information Security Assessment Approach	12
PwC's Assessment of the Twitter Information Security Program, Pursuant to Part III Subparts A, B, C and D of the Order	17
Twitter's Information Security Program Safeguards and PwC's Tests of Effectiveness	27
Management's Assertion	87
Appendix A – Assessment Interviews Summary	88

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



Introduction

Twitter and the Federal Trade Commission entered into the Agreement Containing Consent Order File No: 0923093 ("the Order"), which was served on March 16, 2011.

Part II of the Order requires Twitter to establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information.

Part III of the Order requires Twitter to obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Twitter engaged PricewaterhouseCoopers LLP ("PwC") to perform this biennial assessment.

As described on pages 6-11, Twitter established its information security program by implementing administrative, technical, and physical safeguards to meet or exceed the protections required by Part II of the Order. As described on pages 12-16, PwC performed inquiry, observation, and inspection/examination procedures to assess the effectiveness of the Twitter administrative, technical, and physical control activities implemented to meet or exceed the protections required by Part II of the Order, and our conclusions are on pages 4-5.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



Report of Independent Accountants

To the Management of Twitter, Inc.:

We have examined the accompanying management assertion of Twitter Inc. ("Twitter" or "the Company") that for the two years ended September 12, 2017 (the "Reporting Period"), in accordance with Parts II and III of the Agreement Containing Consent Order ("the Order"), with an effective date of March 16, 2011 between Twitter, Inc. and the United States of America, acting upon notification and authorization by the Federal Trade Commission ("FTC"), the Company had established and implemented a comprehensive Information Security Program ("the Twitter Information Security Program") that is based on the International Organization for Standardization ("ISO") / International Electrotechnical Commission ("IEC") Standard 27002:2013 ("ISO/IEC 27002:2013"), and additional Company specific criteria (collectively referred to as the "Twitter Information Security Program"); and the Twitter Information Security Program was operating with sufficient effectiveness to provide reasonable assurance that the security, privacy, confidentiality, and integrity of nonpublic consumer information collected from or about consumers is protected, and the program has so operated throughout the Assessment Period. The Twitter Information Security Program described in Management's Assertion includes Control Objective #19, which describes the applicable safeguards related to integrating acquired entities during the Reporting Period. Control Objective #19 appropriately did not operate during the Reporting Period because there were no relevant acquisitions made during the Reporting Period. Relevant acquisitions that occurred in prior reporting periods were addressed in prior reports. Over the course of this Reporting Period, Twitter implemented and enhanced controls specific to the products acquired through previous acquisitions, when appropriate, to account for product evolution and changes to their environments.

The Company's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing and extent of the procedures selected depend on our judgment, including an

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are not responsible for Twitter's interpretation of, or compliance with, information security or privacy-related laws, statutes, and regulations applicable to Twitter in the jurisdictions within which Twitter operates. We are also not responsible for Twitter's interpretation of, or compliance with, information security or privacy-related self-regulatory frameworks. Therefore, our examination did not extend to the evaluation of Twitter's interpretation of, or compliance with, information security or privacy-related laws, statutes, regulations, and self-regulatory frameworks with which Twitter has committed to comply.

In our opinion, the Twitter Information Security Program was operating with sufficient effectiveness to provide reasonable assurance that the security, privacy, confidentiality, and integrity of nonpublic consumer information collected from or about consumers was protected, in all material respects, for the two years ended September 12, 2017, based upon the Twitter Information Security Program set forth in Management's Assertion.

(b)(4); (b)(3):6(f)

This report is intended solely for the information and use of the management of Twitter and the United States Federal Trade Commission and is not intended to be and should not be used by anyone other than the specified parties.

PricewaterhouseCoopers LLP

San Jose, California
November 15, 2017

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



Twitter Information Security Program Overview

Company Overview

Twitter is a real-time information network that connects users to the latest information about what they find interesting. Twitter users find the public streams they find most compelling and “follow” the conversations. At the heart of Twitter are small bursts of information called “Tweets,” each Tweet being 140 characters in length or less (in November 2017, the character limit was increased to 280). Twitter users follow the Tweets of other users. Twitter maintains a very high-velocity Internet service, facilitating the transmission currently of approximately half of a billion Tweets per day. As of September 2017, there are 332 million active user accounts on Twitter. Twitter uses an internally-built software infrastructure hosted on multiple machines at several US data centers. Twitter has its primary data center in Sacramento, California and a secondary data center in Atlanta, GA.

Twitter, as a company, had only 29 employees in January 2009. At the beginning of 2011, it had approximately 350 employees, and, in September 2013, it had approximately 2,300 employees. As of September 2015, Twitter had approximately 4,200 employees. As of September 2017, Twitter had approximately 3,500 employees.

Twitter users provide limited profile information, most of which is displayed publicly to all users. When a user creates a Twitter account, the user provides a name, a username, a password, and either an email address, mobile phone number or both. The user may optionally provide a short biography, a location, or a picture. Most of the above information, including the name, username, biography, location, and picture, is listed publicly on the Twitter service.

With regard to the messages sent and received by a user, the majority of these, again, are public. When a user sends a Tweet, it is shared with followers and the rest of the world instantly. Although the default is to make the information public, Twitter does provide settings that allow the Tweets to be “protected”, meaning that the Tweets are shared only with the user’s approved followers.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



Also, Twitter provides the capability to send a "Direct Message" or "DM" which is a personal message sent via Twitter to other Twitter users. The Direct Message is not viewable by users who are not the Direct Message recipient(s).

(b)(4); (b)(3):6(f)

Twitter Information Security Program Governance

The Twitter Information Security Team is responsible for managing overall information security as well as conducting security reviews of different systems across Twitter. The Information Security Team is led by the Chief Information Security Officer, who reports to the SVP of Engineering. The Chief Information Security Officer is responsible for leading the Security Committee, the security training and awareness program, updating and communicating security policy changes, and forming and enforcing the Company's security policies.

The Information Security Team includes Enterprise Security, Platform Security and Security Risk Management and coordinates with related teams to ensure effective operation of the Twitter's Information Security Program. For example, network security is handled by the Network Engineering Team, which is part of Infrastructure Operations. Additionally, Twitter has established a Security Committee which comprises representatives from Security, Trust & Safety, Engineering, Internal Audit, and Legal. The Committee meets formally on a quarterly basis to review the Information Security Program. These reviews can include, amongst other things,

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



reviewing changes to the scope of the program as a result of new products/features, acquisitions, third party arrangements, and changes to internal and external risks; reviewing and updating security policies, training and awareness programs, and roles and responsibilities of the Information Security Teams; reviewing security events; discussing relevant updates from the Legal Team; and reviewing the results of security controls testing performed.

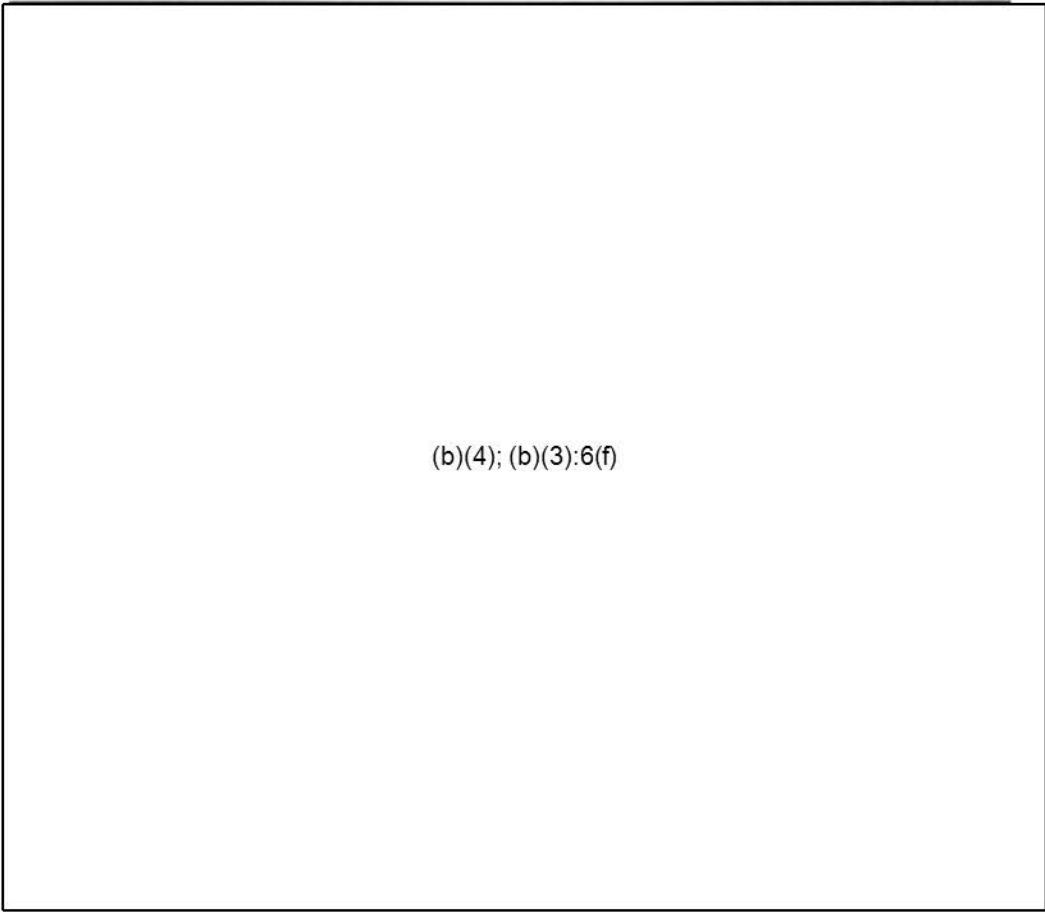
Twitter Information Security Program Scope

Twitter has one primary product/service offering, namely the Twitter service. Accordingly, the relevant business/product scoping is the Twitter service for purposes of the Order. To further define the scope of Twitter's Information Security Program for purposes of the Order, Twitter continuously performs a risk assessment, as described below, using the ISO/IEC 27002:2013 framework. As part of its ongoing risk assessment process, Twitter considers the size, complexity, nature and scope of activities, and amount and nature of nonpublic personal information it collects from or about consumers and adjusts its security program in light of changes to its business. Additional details regarding Twitter's risk assessment process are described in the section below.

Risk Assessment Process

(b)(4); (b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3):6(f)

Data Classification

As part of the ongoing Twitter risk assessment process, the following data types on Twitter information systems are determined as being within the scope of the Order.

(b)(4); (b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.





(b)(4); (b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



PwC's Information Security Assessment Approach

PwC's Assessment Standards

Part III of the Order requires that the Assessments be performed by a qualified, objective, independent third-party professional, who uses procedures and standards that are generally accepted in the profession. This report was issued by PwC under professional standards which meet these same requirements.

As a public accounting firm, PwC must comply with the public accounting profession's technical and ethical standards, which are enforced through various mechanisms created by the American Institute of Certified Public Accountants ("AICPA"). Membership in the AICPA requires adherence to the Institute's Code of Professional Conduct. The AICPA's Code of Professional Conduct and its enforcement are designed to ensure that members of the AICPA accept and achieve a high level of responsibility to the public, clients, and colleagues. The AICPA Professional Standards provide the discipline and rigor required to ensure engagements performed consistently follow specific General Standards, Standards of Fieldwork, and Standards of Reporting ("Standards").

In order to accept and perform this FTC assessment ("engagement"), the Standards state that PwC, as a practitioner, must meet specific requirements, such as the following.

General Standards:

- Have reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users. Suitable criteria must be free from bias (objective), permit reasonably consistent measurements, qualitative or quantitative, of subject matter (measurable), be sufficiently complete so that those relevant factors that would alter a conclusion about subject matter are not omitted (complete), and be relevant to the subject matter;
- Have adequate technical training and proficiency to perform the engagement;
- Have adequate knowledge of the subject matter; and
- Exercise due professional care in planning and performance of the engagement and the preparation of the report.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



Standards of Fieldwork:

- Adequately plan the work and properly supervise any assistants; and
- Obtain sufficient evidence to provide a reasonable basis for the conclusion that is expressed in the report.

Standards of Reporting:

- Identify the assertion being reported on in the report; and
- State the practitioner's conclusion about the assertion in relation to the criteria.

In performing this assessment, PwC complied with all of these Standards.

Independence

The Standards also require PwC to maintain independence in the performance of professional services. Independence requirements fall into five categories: personal financial interests; business relationships; employment relationships; prohibited services; prohibition from serving in the Company's management capacity; and independence in mental attitude. In summary, relevant individuals must not have personal financial interests in the Company; the Company and the Assessor may not have certain business relationships; there are restrictions on relationships that may exist between employees performing the assessment and employees at the Company or formerly at the Company or at the Assessor firm; there are numerous services that cannot be provided by the Assessor to the Company; and the Assessor may not act in a management capacity or make any decisions for the Company.

Further, the Standards require us to maintain independence in mental attitude in all matters relating to the engagement. Independence in mental attitude means there is an objective consideration of facts, unbiased judgments, and honest neutrality on the part of the practitioner in forming and expressing conclusions. We are required to maintain intellectual honesty and impartiality necessary to reach an objective and unbiased conclusion.

PwC is independent with respect to the Standards required for this engagement.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



PwC Assessor Qualifications

(b)(4); (b)(3):6(f)

PwC Assessment Process Overview

(b)(4); (b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



PwC's Assessment of the Twitter Information Security Program, Pursuant to Part III Subparts A, B, C and D of the Order

The table on pages 27-86 details the controls of the Twitter Information Security Program referenced in the Management Assertion on page 87. The Twitter Information Security Program is based on ISO/IEC 27002:2013. Twitter established its Information Security Program by implementing administrative, technical, and physical safeguards to meet or exceed the protections required by Part II of the Order. The table also includes PwC's inquiry, observation, and inspection/examination test procedures to assess the effectiveness of Twitter's Information Security Program and test results. PwC's final conclusions are detailed on pages 4-5 of this document.

Based on PwC's assessment procedures outlined above, the following section summarizes PwC's responses to parts A, B, C and D of Part II of the Order.

A. Set forth the administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period.

The table on pages 27-86 includes a full list of Twitter's administrative, technical, and physical safeguards/controls which have been implemented and maintained by Twitter to meet or exceed the protections required by Part II of the Order. The table includes PwC's test procedures to assess the effectiveness of each safeguard as well as the results of such tests.

B. Explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the nonpublic personal information collected from or about consumers.

As detailed on pages 6-11 of this report, Twitter selected the ISO/IEC 27002:2013 standard, which is an information security standard published by the International Organization for Standardization ("ISO") and the International Electrotechnical Commission ("IEC") as the framework on which they based their Information Security Program (ISO/IEC 27002:2013).

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



ISO/IEC 27002:2013 is a widely adopted industry standard used by companies of all sizes, industries and complexities. It establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management programs, and the objectives outlined in the standard provide general guidance on the commonly accepted goals of information security management. The ISO/IEC 27002:2013 standard is designed to provide a broad set of security risks and illustrative control activities for organizations to consider based on each organization's industry, business practices, size and complexity. It is not designed to be a prescriptive implementation guide, but rather, is based on the underlying principle that the organization should conduct a security risk assessment to identify, quantify and prioritize risks against criteria (i.e., ISO/IEC 27002:2013 criteria) that are relevant to the organization. The results of the risk assessment are meant to guide the organization in the determination of appropriate actions and priorities for managing the relevant information security risks and for designing and implementing customized safeguards to protect against the identified risks.

To evaluate Twitter's information security risk assessment process and its design and implementation of controls to mitigate the risks identified from the risk assessment, as well as the appropriateness of applying ISO/IEC 27002:2013 to Twitter's information security environment, PwC designed and performed the following procedures.

- Inquired of the Security Committee personnel to understand and assess the design of Twitter's methodology and process for conducting its risk assessment.
- Assessed the suitability of the framework selected by Twitter as the basis for its framework (ISO/IEC 27002:2013).
- Assessed the safeguards identified by Twitter to address the risks and selected criteria from the ISO/IEC 27002:2013 to determine whether the safeguards addressed the relevant risks and criteria and aligned with ISO/IEC 27002:2013 guidance as appropriate.
- Performed walkthroughs of the safeguards to assess the design of safeguards to mitigate the relevant security risk and to confirm the safeguards had been placed in operation. Walkthrough procedures consisted of interviewing personnel involved in the execution of the processes (e.g., security management and governance, policy management, asset management, human resource security, physical security, communications and operations management, access management, product and systems development and implementation, incident management, compliance management, etc.) and performing observation and/or inspection procedures, with the interviewees, to validate the design and implementation of the safeguards to address the relevant security risks within the processes.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



C. Explain how the safeguards that have been implemented meet or exceed the protections required by Part II of the order.

Twitter has implemented the safeguards below to meet or exceed the protections required by Part II of the Order. The table on pages 27-86 includes a full list of Twitter's administrative, technical, and physical safeguards/controls which have been implemented and maintained by Twitter to meet or exceed the protections required by Part II of the Order. The safeguards were designed by Twitter based on the ISO/IEC 27002:2013 framework as well as the results of Twitter's continuous risk assessment process. The following paragraphs describe how the safeguards meet or exceed the protections required by Part II of the Order.

A. Designation of an employee or employees to coordinate and be accountable for the program

(b)(4); (b)(3):6(f)

B. The identification of reasonably-foreseeable material risks, both internal and external, that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of nonpublic consumer information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (a) employee training and management; (b) information systems, including network and software design, information processing, storage, transmission, and disposal; and (c) prevention, detection, and response to attacks, intrusions, or other systems failures.

(b)(4); (b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



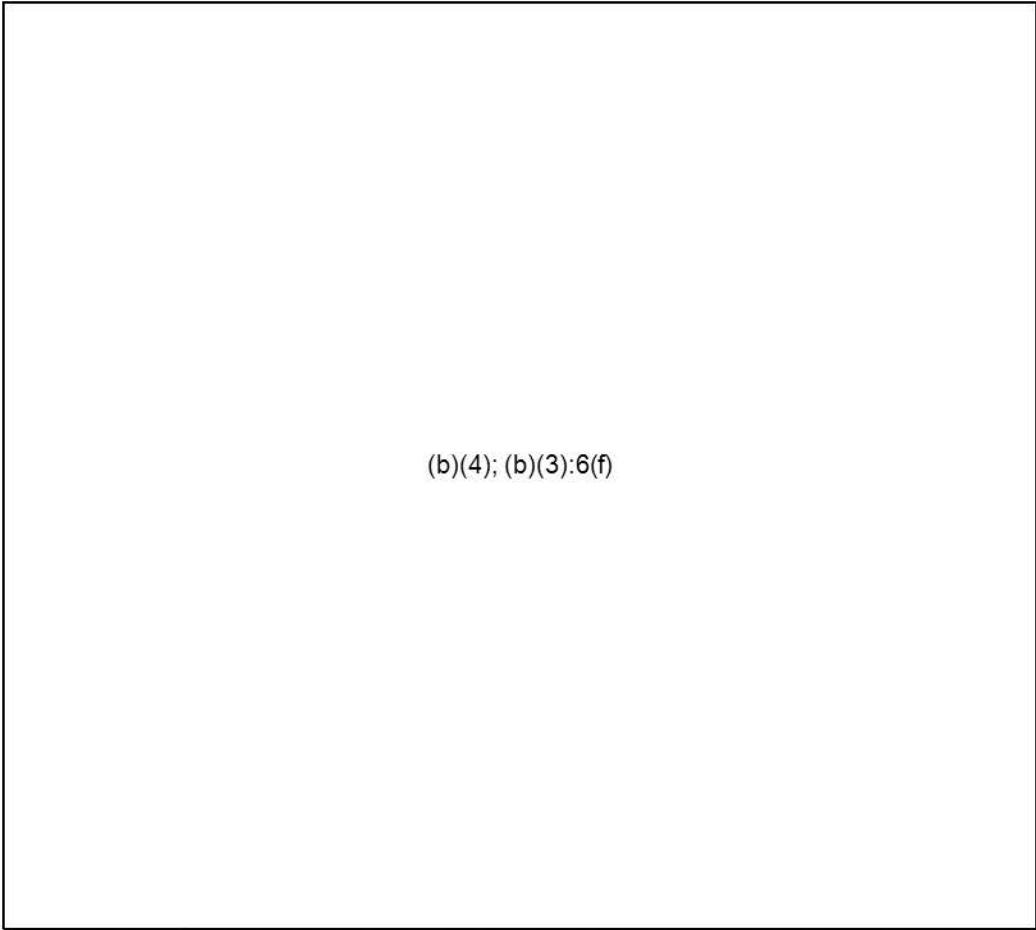
(b)(4); (b)(3):6(f)

C. Design and implementation of reasonable safeguards to control risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems and procedures.

The Twitter Information Security Program includes the design and implementation of reasonable safeguards to control the risks identified through the risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.

(b)(4); (b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3):6(f)

The table on pages 27-86 also describes PwC's assessment of the safeguards the Company has identified and maintained to monitor the Twitter Information Security Program.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



D. The development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding nonpublic consumer information such service providers receive from respondent or obtain on respondent's behalf, and the requirement, by contract, that such service providers implement and maintain appropriate safeguards, provided, however that this subparagraph shall not apply to personal information about a consumer that respondent provides to a government agency or lawful information supplier when the agency or supplier already possesses the information and uses it only to retrieve and supply to respondent, additional personal information about the consumer.

The Twitter Information Security Program includes the design and implementation of reasonable steps to select and retain service providers capable of appropriately safeguarding nonpublic consumer information the service providers receive from Twitter or obtain on Twitter's behalf.

(b)(4); (b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3):6(f)

The table on pages 27-86 also describes PwC's assessment of the safeguards the Company has identified and maintained to select and retain service providers as part of the Twitter Information Security Program.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



E. The evaluation and adjustment of Defendant's information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to Defendant's operations or business arrangements, or any other circumstances that Defendant knows or has reason to know may have a material impact on the effectiveness of its information security program.

(b)(4); (b)(3):6(f)

The table on pages 27-86 also describes PwC's assessment of the safeguards the Company has identified and maintained evaluate and adjust the Twitter Information Security Program in light of the results of testing and monitoring and any material changes to its operation.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



D. Certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information and that the program has so operated throughout the reporting period.

As described in the PwC Assessment Overview section above, PwC performed its assessment of Twitter's information security program in accordance with AICPA Attestation Standards Section 205, AT-C 205 Engagements. Refer to pages 4-5 above for PwC's conclusions.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



Twitter's Information Security Program Safeguards and PwC's Tests of Effectiveness

Provided below are Twitter's Information Security Program Safeguards and PwC's Tests of Effectiveness. Also provided are the results of the testing performed by PwC. Finally, additional information has been provided by PwC for the instances in which PwC identified an exception during testing. This information is provided in an effort to enhance the FTC's understanding of the exception.

Note: Controls that end in .V apply to the Vine environment only and operated from the start of the Reporting Period through the decommissioning of the application and related production environment. Controls that end in .T apply to the TCDC environment only and operated from the date of the Vine transition to TCDC through end of the Reporting Period. Controls that end in .P apply to the Periscope environment only and were introduced as appropriate taking into consideration product evolution and changes to the environment during the course of the Reporting Period.

ISO Ref	ISO Control Objective Description	Twitter Safeguard Description	Type of Safeguard	PwC's Test of Effectiveness	PwC's Test Results	Additional Information
(b)(4); (b)(3):6(f)						

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3); 6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

0

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)



Independent Assessor's Report on Twitter, Inc.'s Information Security Program

For the period September 13, 2017 – September 12, 2019

The contents of this document, including the Report of Independent Accountants, contain PricewaterhouseCoopers LLP proprietary information that shall be protected from disclosure outside of the U.S. Government in accordance with the U.S. Trade Secrets Act and Exemption 4 of the U.S. Freedom of Information Act (FOIA). The document constitutes and reflects work performed or information obtained by PricewaterhouseCoopers LLP, in our capacity as independent assessor for Twitter, Inc. for the purpose of the Twitter, Inc. Order. The document contains proprietary information, trade secrets and confidential commercial information of our firm and Twitter, Inc. that is privileged and confidential, and we expressly reserve all rights with respect to disclosures to third parties. Accordingly, we request confidential treatment under the Freedom of Information Act (FOIA), the U.S. Trade Secrets Act or similar laws and regulations when requests are made for the report or information contained therein or any documents created by the FTC containing information derived from the report. We further request that written notice be given to PwC and Twitter, Inc. before distribution of the information in the report (or copies thereof) to others, including other governmental agencies, to afford our firm and Twitter, Inc. with the right to assert objections and defenses to the release of the information as permitted under FOIA or other similar applicable law or regulation, except when such distribution is already required by law or regulation. This report is intended solely for the information and use of the management of Twitter, Inc. and the U.S. Federal Trade Commission and is not intended to be and should not be used by anyone other than these specified parties.



Table of Contents

Introduction	3
Report of Independent Accountants	4
Twitter Information Security Program Overview	6
PwC's Information Security Assessment Approach	12
PwC's Assessment of the Twitter Information Security Program, Pursuant to Part III Subparts A, B, C and D of the Order	17
Twitter's Information Security Program Safeguards and PwC's Tests of Effectiveness	27
Management's Assertion	82
Appendix A – Assessment Interviews Summary	83

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



Introduction

Twitter and the Federal Trade Commission entered into the Agreement Containing Consent Order File No: 0923093 (“the Order”), which was served on March 16, 2011.

Part II of the Order requires Twitter to establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information.

Part III of the Order requires Twitter to obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Twitter engaged PricewaterhouseCoopers LLP (“PwC”) to perform this biennial assessment.

As described on pages 6-11, Twitter established its information security program by implementing administrative, technical, and physical safeguards to meet or exceed the protections required by Part II of the Order. As described on pages 12-16, PwC performed inquiry, observation, and inspection/examination procedures to assess the effectiveness of the Twitter administrative, technical, and physical control activities implemented to meet or exceed the protections required by Part II of the Order, and our conclusions are on pages 4-5.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



Report of Independent Accountants

To the Management of Twitter, Inc.:

We have examined the accompanying management assertion of Twitter Inc. ("Twitter" or the "Company") that for the two years ended September 12, 2019 (the "Reporting Period"), in accordance with Parts II and III of the Agreement Containing Consent Order ("the Order"), with an effective date of March 16, 2011 between Twitter, Inc. and the United States of America, acting upon notification and authorization by the Federal Trade Commission ("FTC"), the Company had established and implemented a comprehensive Information Security Program ("the Twitter Information Security Program") that is based on the International Organization for Standardization ("ISO") / International Electrotechnical Commission ("IEC") Standard 27002:2013 ("ISO/IEC 27002:2013"), and additional Company specific criteria (collectively referred to as the "Twitter Information Security Program"); and the Twitter Information Security Program was operating with sufficient effectiveness to provide reasonable assurance that the security, privacy, confidentiality, and integrity of nonpublic consumer information collected from or about consumers is protected, and the program has so operated throughout the Reporting Period. The Twitter Information Security Program described in Management's Assertion includes Control Objective #19, which describes the applicable safeguards related to integrating acquired entities during the Reporting Period. Control Objective #19 appropriately did not operate during the Reporting Period because there were no relevant acquisitions made during the Reporting Period. Over the course of this Reporting Period, Twitter implemented and enhanced controls specific to the products acquired through previous acquisitions, when appropriate, to account for product evolution and changes to their environments.

The Company's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



We are not responsible for Twitter's interpretation of, or compliance with, information security or privacy-related laws, statutes, and regulations applicable to Twitter in the jurisdictions within which Twitter operates. We are also not responsible for Twitter's interpretation of, or compliance with, information security or privacy-related self-regulatory frameworks. Therefore, our examination did not extend to the evaluation of Twitter's interpretation of, or compliance with, information security or privacy-related laws, statutes, regulations, and self-regulatory frameworks with which Twitter has committed to comply.

In our opinion, the Twitter Information Security Program was operating with sufficient effectiveness to provide reasonable assurance that the security, privacy, confidentiality, and integrity of nonpublic consumer information collected from or about consumers was protected, in all material respects, for the two years ended September 12, 2019, based upon the Twitter Information Security Program set forth in Management's Assertion.

(b)(4);
(b)(3):6(f)

This report is intended solely for the information and use of the management of Twitter and the United States Federal Trade Commission and is not intended to be and should not be used by anyone other than the specified parties.

PricewaterhouseCoopers LLP

San Francisco, California
November 11, 2019

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



Twitter Information Security Program Overview

Company Overview

Twitter is a real-time information network that connects users to the latest information about what they find interesting. Twitter users find the public streams they find most compelling and “follow” the conversations. At the heart of Twitter are small bursts of information called “Tweets,” each Tweet being 280 characters in length or less (in November 2017, the character limit was increased from 140 to 280). Twitter users follow the Tweets of other users. Twitter maintains a very high-velocity Internet service, facilitating the transmission currently of approximately half of a billion Tweets per day. As of September 2019, there are 145 million monetizable daily active users on Twitter. Twitter uses an internally-built software infrastructure hosted on multiple machines at several US data centers. Twitter has its primary data center in Sacramento, California and a secondary data center in Atlanta, GA.

Twitter, as a company, had only 29 employees in January 2009. At the beginning of 2011, it had approximately 350 employees, and, in September 2013, it had approximately 2,300 employees. As of September 2015, Twitter had approximately 4,200 employees. As of September 2017, Twitter had approximately 3,500 employees. As of September 2019, Twitter had approximately 4,500 employees.

Twitter users provide limited profile information, most of which is displayed publicly to all users. When a user creates a Twitter account, the user provides a name, a username, a password, and either an email address, mobile phone number or both. The user may optionally provide a short biography, a location, or a picture. Most of the above information, including the name, username, biography, location, and picture, is listed publicly on the Twitter service.

With regard to the messages sent and received by a user, the majority of these, again, are public. When a user sends a Tweet, it is shared with followers and the rest of the world instantly. Although the default is to make the information public, Twitter does provide settings that allow the Tweets to be “protected,” meaning that the Tweets are shared only with the user’s approved followers. Also, Twitter provides the capability to send a “Direct Message” or “DM” which is a personal message sent via Twitter to other Twitter users. The Direct Message is not viewable by users who are not the Direct Message recipient(s).

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3); 6(f)

Twitter Information Security Program Governance

The mission of the Information Security organization is to secure Twitter's products and sensitive data. The team accomplishes this through a variety of service channels that range from architecting and development of security infrastructure, vulnerability management, policy, internal security consulting, incident response, risk management, training and awareness, application security, and third-party security / M&A due diligence. The Information Security team is led by a Chief Information Security Officer; over the course of the past 2 years (Sept 2017 - Sept 2019) that role was filled on an interim basis by Joseph Camilleri, Director Security Risk Management, until November 2018 when Mike Convertino was hired as the Twitter's full-time CISO. The CISO reports to Michael Montano, Head of Engineering/Member of Staff, who reports to Jack Dorsey, Chief Executive Officer.

Information Security objectives are included in our company-wide planning process and include major initiatives (new) and run the business security activities. InfoSec specific progress on our objectives are tracked by the CISO and reported to Senior Management at periodic intervals. On an annual basis InfoSec produces a holistic Information Security Risk Assessment and shares results with relevant internal oversight groups including but not limited to Legal, Compliance, Members of Security Committee, Internal Audit, etc. On a quarterly basis, the CISO hosts a Security Committee session to discuss security trends, top risks / their treatment, rising risks, and a look back of security incidents during the last 90 days. The membership of Security Committee includes leadership from Information Security, Engineering, Legal, Internal Audit, Corporate Security, and other invited guests as necessary.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3); 6(f)

Twitter Information Security Program Scope

Twitter has one primary product/service offering, namely the Twitter service. Accordingly, the relevant business/product scoping is the Twitter service for purposes of the Order. To further define the scope of Twitter's Information Security Program for purposes of the Order, Twitter continuously performs a risk assessment, as described below, using the ISO/IEC 27002:2013 framework. As part of its ongoing risk assessment process, Twitter considers the size, complexity, nature and scope of activities, and amount and nature of nonpublic personal information it collects from or about consumers and adjusts its security program in light of changes to its business. Additional details regarding Twitter's risk assessment process are described in the section below.

Risk Assessment Process

(b)(4); (b)(3); 6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3); 6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3); 6(f)

Data Classification

As part of the ongoing Twitter risk assessment process, the following data types on Twitter information systems are determined as being within the scope of the Order.

(b)(4); (b)(3); 6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3); 6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



PwC's Information Security Assessment Approach

PwC's Assessment Standards

Part III of the Order requires that the Assessments be performed by a qualified, objective, independent third-party professional, who uses procedures and standards that are generally accepted in the profession. This report was issued by PwC under professional standards which meet these same requirements.

As a public accounting firm, PwC must comply with the public accounting profession's technical and ethical standards, which are enforced through various mechanisms created by the American Institute of Certified Public Accountants ("AICPA"). Membership in the AICPA requires adherence to the Institute's Code of Professional Conduct. The AICPA's Code of Professional Conduct and its enforcement are designed to ensure that members of the AICPA accept and achieve a high level of responsibility to the public, clients, and colleagues. The AICPA Professional Standards provide the discipline and rigor required to ensure engagements performed consistently follow specific General Standards, Standards of Fieldwork, and Standards of Reporting ("Standards").

In order to accept and perform this FTC assessment ("engagement"), the Standards state that PwC, as a practitioner, must meet specific requirements, such as the following.

General Standards:

- Have reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users. Suitable criteria must be free from bias (objective), permit reasonably consistent measurements, qualitative or quantitative, of subject matter (measurable), be sufficiently complete so that those relevant factors that would alter a conclusion about subject matter are not omitted (complete), and be relevant to the subject matter;
- Have adequate technical training and proficiency to perform the engagement;
- Have adequate knowledge of the subject matter; and
- Exercise due professional care in planning and performance of the engagement and the preparation of the report.

Standards of Fieldwork:

- Adequately plan the work and properly supervise any assistants; and

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



- Obtain sufficient evidence to provide a reasonable basis for the conclusion that is expressed in the report.

Standards of Reporting:

- Identify the assertion being reported on in the report; and
- State the practitioner's conclusion about the assertion in relation to the criteria.

In performing this assessment, PwC complied with all of these Standards.

Independence

The Standards also require PwC to maintain independence in the performance of professional services. Independence requirements fall into six categories: personal financial interests; business relationships; employment relationships; prohibited services; prohibition from serving in the Company's management capacity; and independence in mental attitude. In summary, relevant individuals must not have personal financial interests in the Company; the Company and the Assessor may not have certain business relationships; there are restrictions on relationships that may exist between employees performing the assessment and employees at the Company or formerly at the Company or at the Assessor firm; there are numerous services that cannot be provided by the Assessor to the Company; and the Assessor may not act in a management capacity or make any decisions for the Company.

Further, the Standards require us to maintain independence in mental attitude in all matters relating to the engagement. Independence in mental attitude means there is an objective consideration of facts, unbiased judgments, and honest neutrality on the part of the practitioner in forming and expressing conclusions. We are required to maintain intellectual honesty and impartiality necessary to reach an objective and unbiased conclusion.

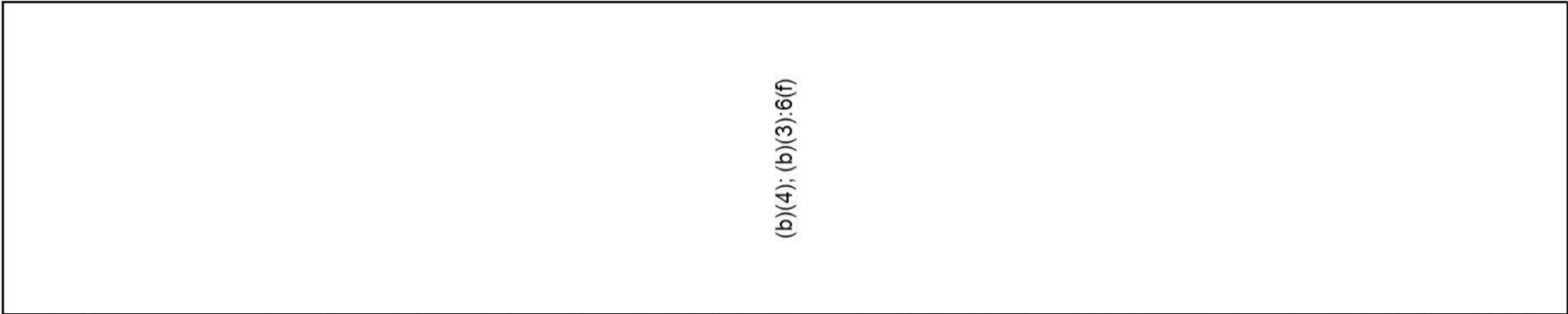
PwC is independent with respect to the Standards required for this engagement.

PwC Assessor Qualifications

[Redacted]

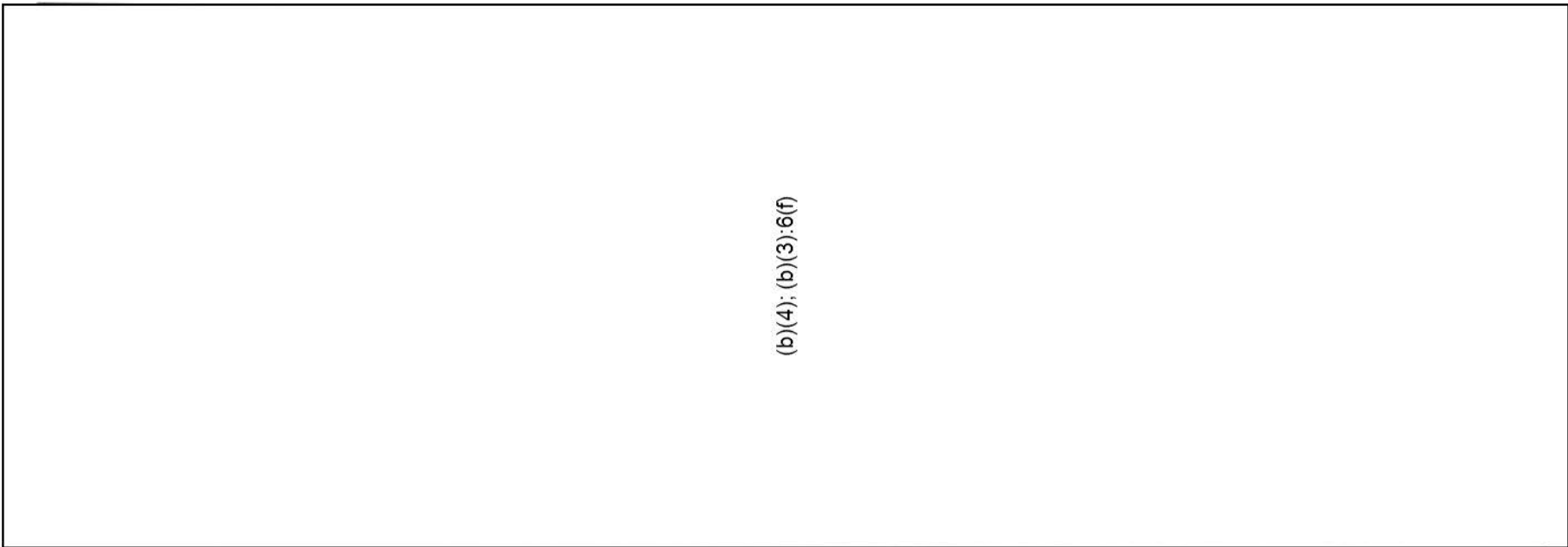
(b)(4);
(b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



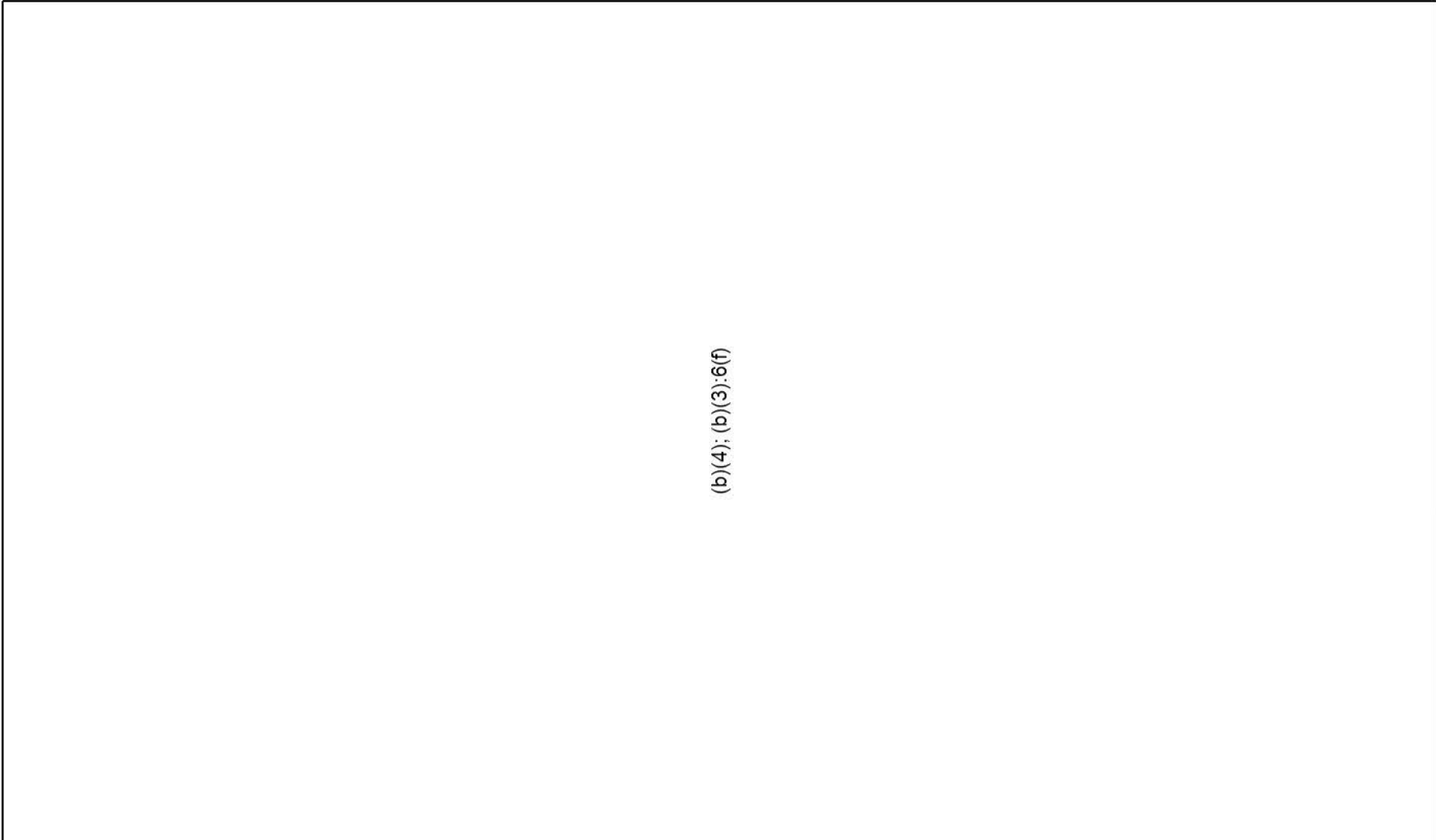
(b)(4); (b)(3):6(f)

PwC Assessment Process Overview



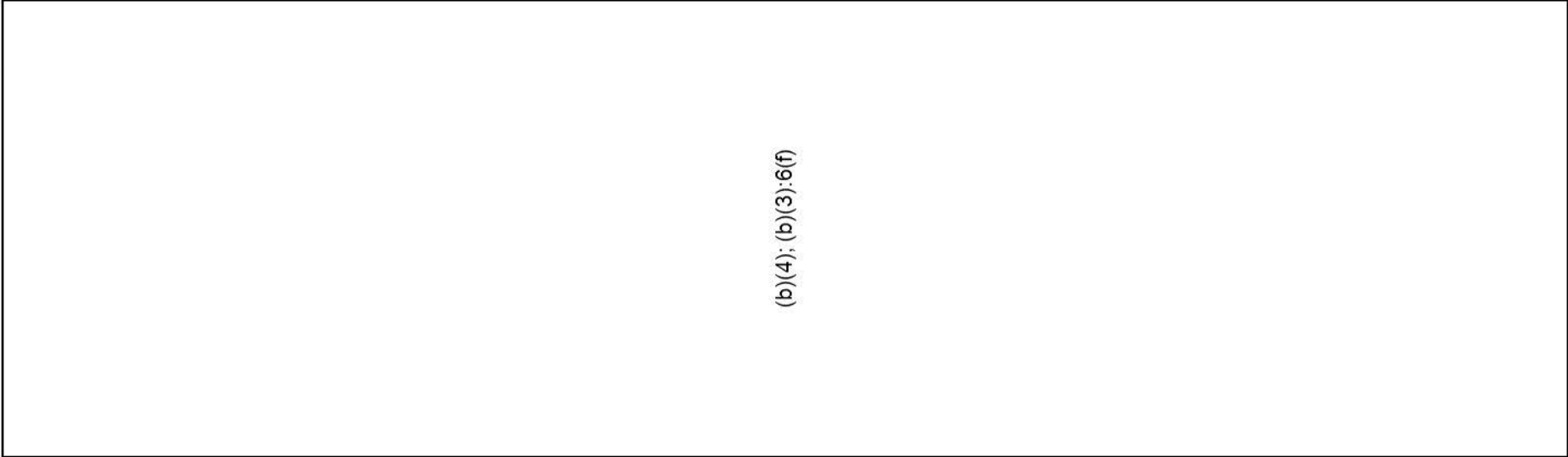
(b)(4); (b)(3):6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3); 6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3); 6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



PwC's Assessment of the Twitter Information Security Program, Pursuant to Part III Subparts A, B, C and D of the Order

The table on pages 27-81 details the controls of the Twitter Information Security Program referenced in the Management Assertion on page 82. The Twitter Information Security Program is based on ISO/IEC 27002:2013, and additional Company specific criteria (collectively referred to as the "Twitter Information Security Program"). Twitter established its Information Security Program by implementing administrative, technical, and physical safeguards to meet or exceed the protections required by Part II of the Order. The table also includes PwC's inquiry, observation, and inspection/examination test procedures to assess the effectiveness of Twitter's Information Security Program and test results. PwC's final conclusions are detailed on pages 4-5 of this document.

Based on PwC's assessment procedures outlined above, the following section summarizes PwC's responses to parts A, B, C and D of Part II of the Order.

A. Set forth the administrative, technical, and physical safeguards that respondent has implemented and maintained during the Reporting Period.

The table on pages 27-81 includes a list of Twitter's administrative, technical, and physical safeguards/controls which have been implemented and maintained by Twitter to meet or exceed the protections required by Part II of the Order. The table includes PwC's test procedures to assess the effectiveness of each safeguard as well as the results of such tests.

B. Explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the nonpublic personal information collected from or about consumers.

As detailed on pages 6-11 of this report, Twitter selected the ISO/IEC 27002:2013 standard, which is an information security standard published by the International Organization for Standardization ("ISO") and the International Electrotechnical Commission ("IEC") as the framework on which they based their Information Security Program (ISO/IEC 27002:2013).

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



ISO/IEC 27002:2013 is a widely adopted industry standard used by companies of all sizes, industries and complexities. It establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management programs, and the objectives outlined in the standard provide general guidance on the commonly accepted goals of information security management. The ISO/IEC 27002:2013 standard is designed to provide a broad set of security risks and illustrative control activities for organizations to consider based on each organizations industry, business practices, size and complexity. It is not designed to be a prescriptive implementation guide, but rather, is based on the underlying principle that the organization should conduct a security risk assessment to identify, quantify and prioritize risks against criteria (i.e., ISO/IEC 27002:2013 criteria) that are relevant to the organization. The results of the risk assessment are meant to guide the organization in the determination of appropriate actions and priorities for managing the relevant information security risks and for designing and implementing customized safeguards to protect against the identified risks.

To evaluate Twitter's information security risk assessment process and its design and implementation of controls to mitigate the risks identified from the risk assessment, as well as the appropriateness of applying ISO/IEC 27002:2013 to Twitter's information security environment, PwC designed and performed the following procedures.

- Inquired of the Security Committee personnel to understand and assess the design of Twitter's methodology and process for conducting its risk assessment.
- Assessed the suitability of the framework selected by Twitter as the basis for its framework (ISO/IEC 27002:2013).
- Assessed the safeguards identified by Twitter to address the risks and selected criteria from the ISO/IEC 27002:2013 to determine whether the safeguards addressed the relevant risks and criteria and aligned with ISO/IEC 27002:2013 guidance as appropriate.
- Performed walkthroughs of the safeguards to assess the design of safeguards to mitigate the relevant security risk and to confirm the safeguards had been placed in operation. Walkthrough procedures consisted of interviewing personnel involved in the execution of the processes (e.g., security management and governance, policy management, asset management, human resource security, physical security, communications and operations management, access management, product and systems development and implementation, incident management, compliance management) and performing observation and/or inspection procedures, with the interviewees, to validate the design and implementation of the safeguards to address the relevant security risks within the processes.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



C. Explain how the safeguards that have been implemented meet or exceed the protections required by Part II of the Order.

Twitter has implemented the safeguards below to meet or exceed the protections required by Part II of the Order. The table on pages 27-81 includes a full list of Twitter’s administrative, technical, and physical safeguards/controls which have been implemented and maintained by Twitter to meet or exceed the protections required by Part II of the Order. The safeguards were designed by Twitter based on the ISO/IEC 27002:2013 framework as well as the results of Twitter’s continuous risk assessment process. The following paragraphs describe how the safeguards meet or exceed the protections required by Part II of the Order.

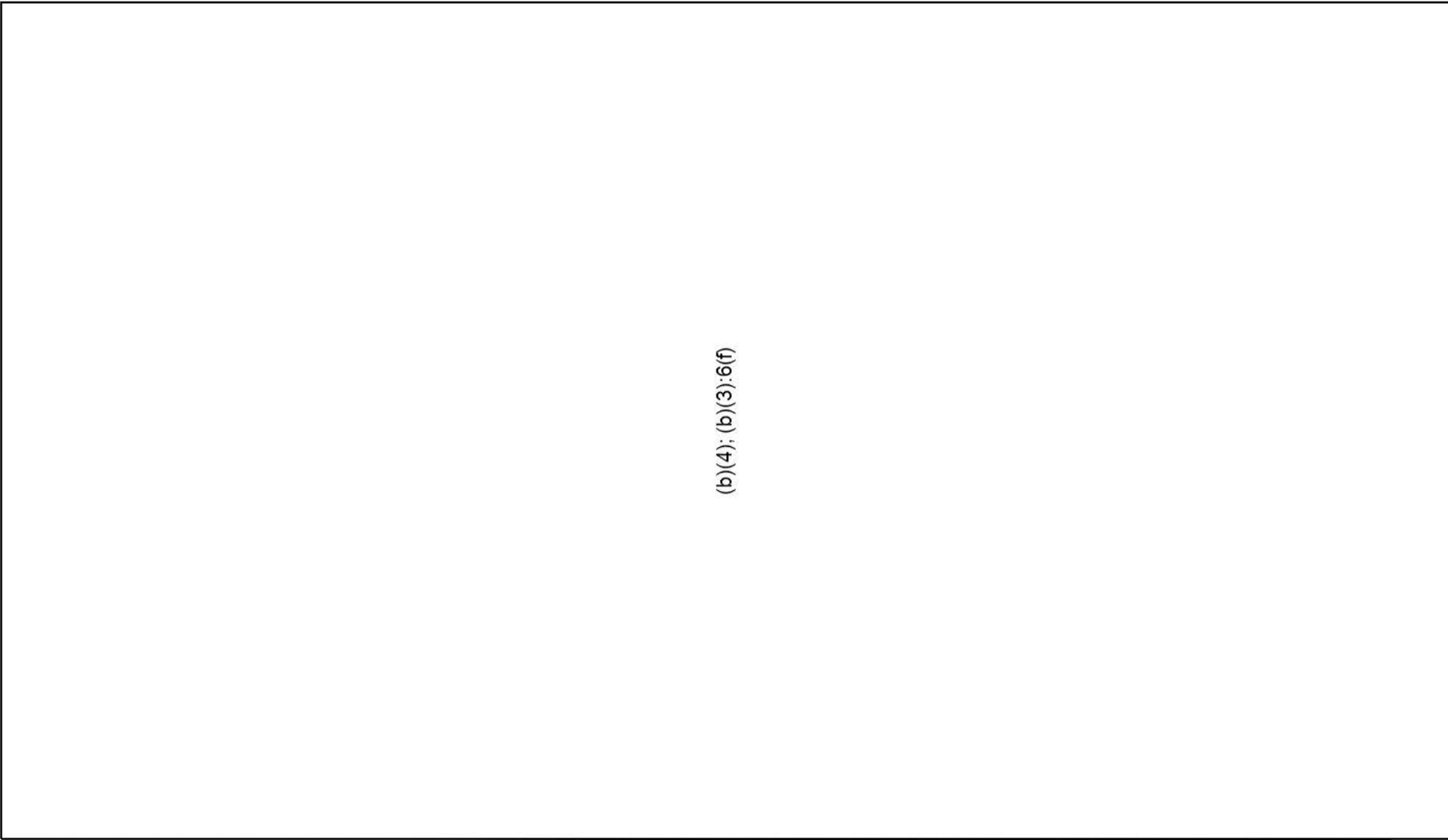
I. Designation of an employee or employees to coordinate and be accountable for the program

(b)(4); (b)(3); 6(f)

II. The identification of reasonably- foreseeable material risks, both internal and external, that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of nonpublic consumer information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (a) employee training and management; (b) information systems, including network and software design, information processing, storage, transmission, and disposal; and (c) prevention, detection, and response to attacks, intrusions, or other systems failures.

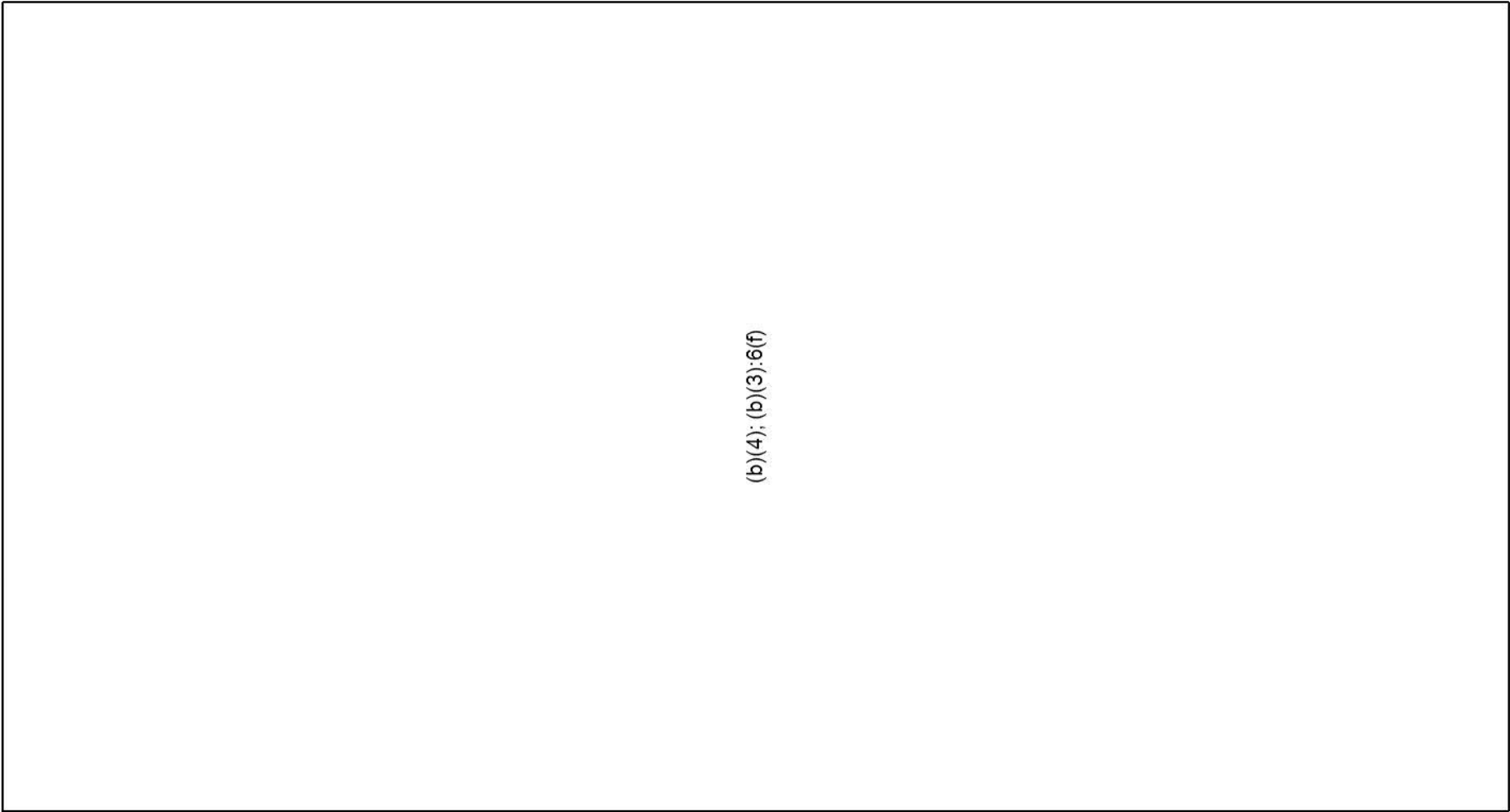
(b)(4); (b)(3); 6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3); 6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



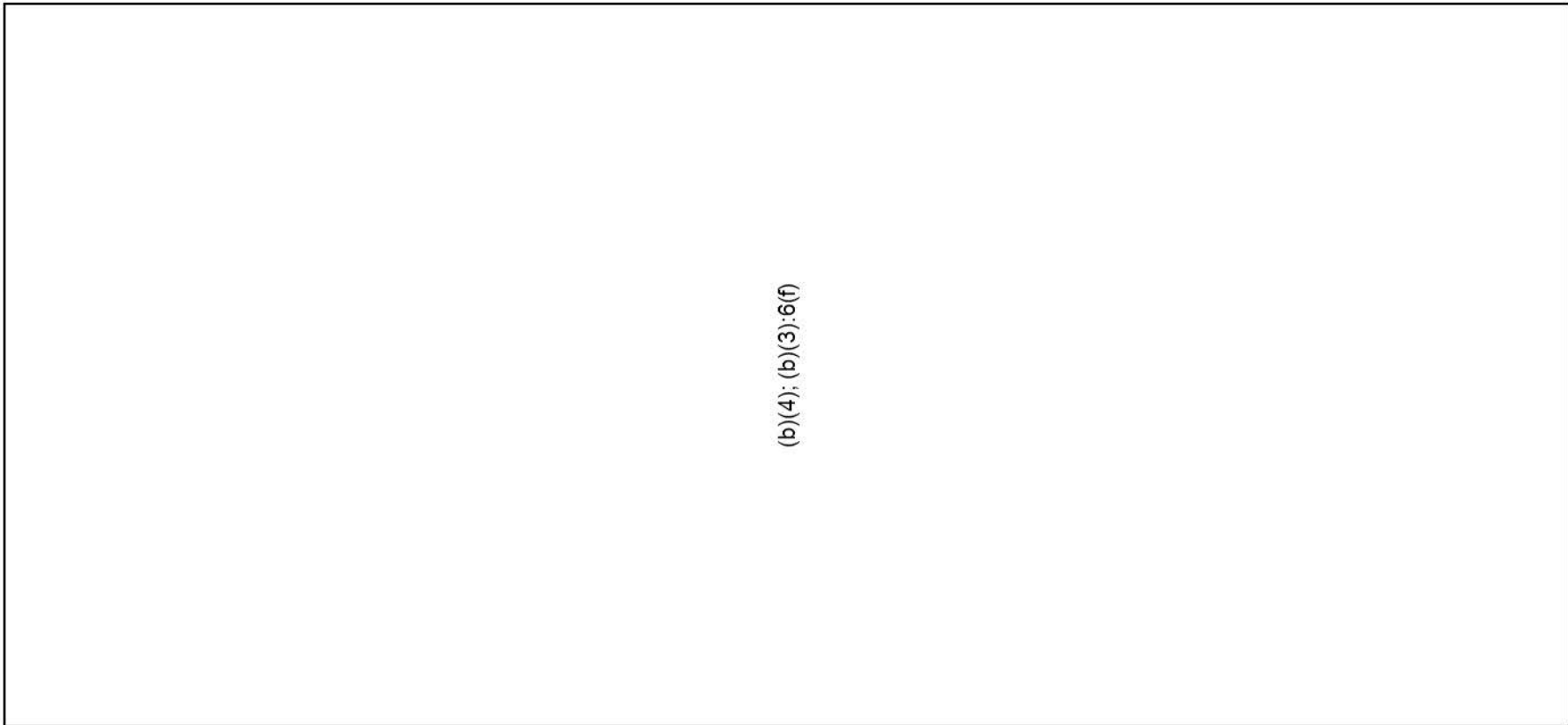
(b)(4); (b)(3); 6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



III. Design and implementation of reasonable safeguards to control risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems and procedures.

The Twitter Information Security Program includes the design and implementation of reasonable safeguards to control the risks identified through the risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.



(b)(4); (b)(3); 6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3); 6(f)

The table on pages 27-81 also describes PwC’s assessment of the safeguards the Company has identified and maintained to monitor the Twitter Information Security Program.

D. The development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding nonpublic consumer information such service providers receive from respondent or obtain on respondent’s behalf, and the requirement, by contract, that such service providers implement and maintain appropriate safeguards, provided, however that this subparagraph shall not apply to personal information about a consumer that respondent provides to a government agency or lawful information supplier when the agency or supplier already possesses the information and uses it only to retrieve and supply to respondent, additional personal information about the consumer.

The Twitter Information Security Program includes the design and implementation of reasonable steps to select and retain service providers capable of appropriately safeguarding nonpublic consumer information the service providers receive from Twitter or obtain on Twitter’s behalf.

(b)(4); (b)(3); 6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3);6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4);
(b)(3);6(f)

The table on pages 27-81 also describes PwC's assessment of the safeguards the Company has identified and maintained to select and retain service providers as part of the Twitter Information Security Program.

E. The evaluation and adjustment of Defendant's information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to Defendant's operations or business arrangements, or any other circumstances that Defendant knows or has reason to know may have a material impact on the effectiveness of its information security program.

(b)(4); (b)(3);6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4);
(b)(3):6(f)

The table on pages 27-81 also describes PwC's assessment of the safeguards the Company has identified and maintained evaluate and adjust the Twitter Information Security Program in light of the results of testing and monitoring and any material changes to its operation.

F. Certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information and that the program has so operated throughout the reporting period.

As described in the PwC Assessment Overview section above, PwC performed its assessment of Twitter's information security program in accordance with AICPA Attestation Standards Section 205, AT-C 205 Engagements. Refer to pages 4-5 above for PwC's conclusions.

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



Twitter's Information Security Program Safeguards and PwC's Tests of Effectiveness

Provided below are Twitter's Information Security Program Safeguards and PwC's Tests of Effectiveness. Also provided are the results of the testing performed by PwC. Finally, additional information has been provided by PwC for the instances in which PwC identified an exception during testing. This information is provided in an effort to enhance the FTC's understanding of the exception.

Note: Controls that end in .G apply to the Google Cloud Platform (GCP) environment only and were in place from the start of Twitter's use of Google Cloud, March 2018, through the end of the Reporting Period. Controls that end in .T apply to the TCDC environment only and were in place throughout the whole Reporting Period. Controls that end in .P apply to the Periscope environment only and were in place throughout the whole Reporting Period.

ISO Ref	ISO Control Objective Description	Twitter Safeguard Description	Type of Safeguard	PwC's Test of Effectiveness	PwC's Test Results	Additional Information
(b)(4); (b)(3);6(f)						

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6f

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3); 6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)

(b)(4); (b)(3):6(f)



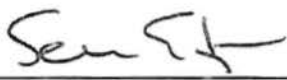
Management's Assertion

The management of Twitter, Inc. ("Twitter" or "the Company") represents that for the two years ended September 12, 2019 ("the Reporting Period"), in accordance with Parts II and III of the Agreement Containing Consent Order ("The Order"), with a service date of March 16, 2011, between Twitter, Inc. and the United States of America, acting upon notification and authorization by the Federal Trade Commission ("FTC"), the Company had established and implemented a comprehensive Information Security Program ("the Twitter Information Security Program"), that is based on the International Organization for Standardization ("ISO") / International Electrotechnical Commission ("IEC") Standard 27002:2013 ("ISO/IEC 27002:2013"), and additional Company specific criteria (collectively referred to as the "Twitter Information Security Program"); and the Twitter Information Security Program was operating with sufficient effectiveness to provide reasonable assurance that the security, privacy, confidentiality, and integrity of nonpublic consumer information collected from or about consumers is protected, and the program has so operated throughout the Reporting Period. The Twitter Information Security Program described in Management's Assertion includes Control Objective #19, which describes the applicable safeguards related to integrating acquired entities during the Reporting Period. Control Objective #19 appropriately did not operate during the Reporting Period because there were no relevant acquisitions made during the Reporting Period. Over the course of this Reporting Period, Twitter implemented and enhanced controls specific to the products acquired through previous acquisitions, when appropriate, to account for product evolution and changes to their environments.

Furthermore, the Company represents that for the Reporting Period, the administrative, technical and physical safeguards within the Twitter Information Security Program are appropriate to its size, complexity, the nature and scope of its activities, and sensitivity of personal information collected from or about consumers.

For additional information provided by the Company regarding the Twitter Information Security Program refer to pages 6-11.

Twitter, Inc.

By: 

Sean Edgett
General Counsel

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.

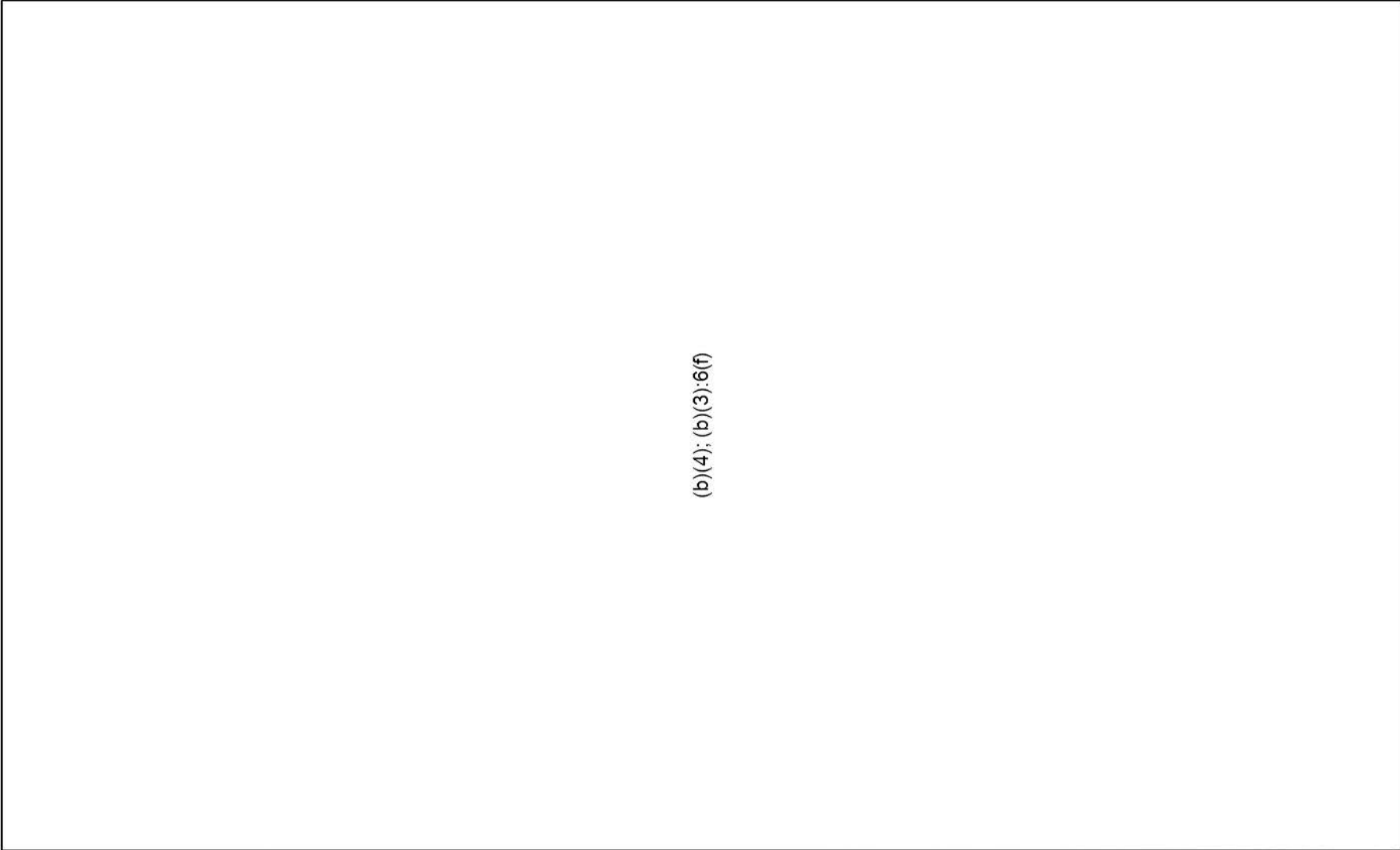


Appendix A – Assessment Interviews Summary

The primary Twitter individuals interviewed by PwC, as a part of the above Assessment procedures, include, but are not limited to, those individuals listed in the table below.

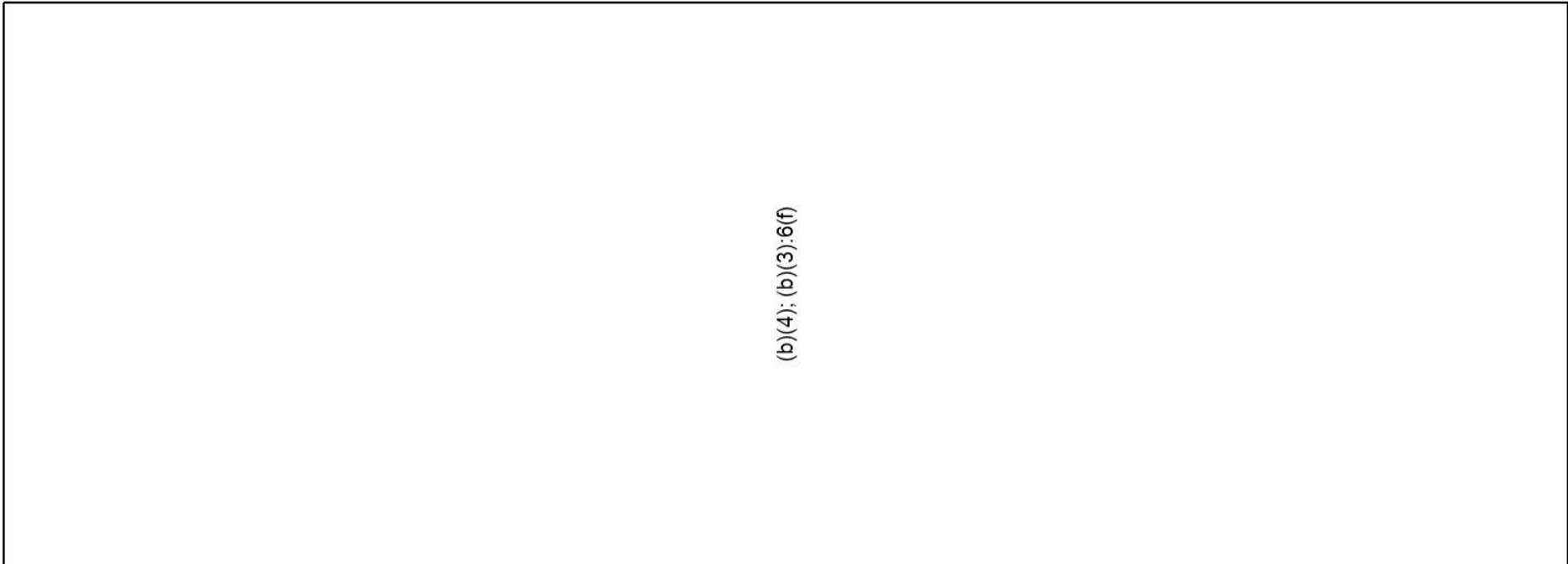
Title	Department
(b)(4); (b)(3); 6(f)	

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3); 6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.



(b)(4); (b)(3); 6(f)

Use or disclosure of data contained on this page is subject to the restriction on the title page of this report.