pwc

February 24, 2012

Mr. Alexander Macgillivray
General Counsel & Secretary, Twitter
795 Folsom Street, Suite 600
San Francisco, CA 94103

Dear Mr. Macgillivray:

PricewaterhouseCoopers ("PwC" or "we" or "our" or "Assessor") is writing this letter in response to the Federal Trade Commission's ("FTC") letter to Twitter, Inc. ("Twitter" or "the Company") from Mr. Waller dated February 9, 2012 titled "re: In the Matter of Twitter, Inc., FTC Docket No. C-4316." The FTC has commented that the Assessment does not address Parts A, B, and C of Paragraph III of the Commission's Decision and Order served on March 16, 2011 Assessment ("Assessment"). In response, in the following pages, we more thoroughly address Parts A, B, and C of Paragraph III.

Should you have any questions or comments related to the procedures performed by PwC as part of our Assessment of Twitter's Information Security Program, please contact Carolyn Holcomb at (678) 419-1696, via e-mail at carolyn.c.holcomb@us.pwc.com, or physical mail at 10 10th St. NW, Suite 1400, Atlanta, GA 30309.

Sincerely,

Carolyn C. Holcomb

Executive Summary

Executive Summary

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. Twitter users follow the Tweets of other users. Twitter maintains a very high-velocity Internet service, facilitating the transmission currently of over a billion Tweets per week. Currently, there are over 200 million user accounts on Twitter. Twitter uses an internally-built software infrastructure hosted on multiple machines at several US data centers. Twitter's primary data center is in Sacramento, California.

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

Paragraph 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.

Paragraph 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 the initial assessment.

As described on pages 3-4, Twitter established its information security program by implementing administrative, technical, and physical safeguards to meet or exceed the protections required by Paragraph II of the Order. As described on pages 6-9, 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 Paragraph II of the Order, and our conclusions are on pages 20-21.

pwc

Twitter Information Security Program & Assessment 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. Twitter users follow the Tweets of other users. Twitter maintains a very high-velocity Internet service, facilitating the transmission currently of over a billion Tweets per week. Currently, there are over 200 million user accounts on Twitter. Twitter uses an internally-built software infrastructure hosted on multiple machines at several US data centers. Twitter's primary data center is in Sacramento, California.

Twitter, as a company, had only 29 employees in January 2009. At the beginning of 2011, it had approximately 350 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 an email address. The user may optionally provide a short biography, a location, or a picture. The user may also include his or her cell phone number for the delivery of SMS messages. Most of the above information is listed publicly on the Twitter service, including the name, username, biography, location, and picture.

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 one of the user's followers. The Direct Message is not viewable by other users.

Twitter Information Security Program Scope

Twitter has only one 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 performed a risk assessment, as described below, using the ISO/IEC 27002:2005 framework.

Risk Assessment Process

The Security Team, in consultation with the Legal Team, met with Engineering, Trust & Safety, HR, Finance, Facilities, and IT team leads at Twitter to conduct a risk assessment of information security practices at Twitter. The objective of the risk assessment was to identify material risks, both internal and external, that could result in the compromise of nonpublic consumer information. After identifying all data types that might constitute nonpublic consumer information, the teams conducted an inventory of the information systems and physical locations at Twitter where the identified data types may reside. The teams made a determination of the material risks, taking into account the nature and scope of Twitter's activities, the sensitivities of the nonpublic information collected, the size of the service, the number of registered users, and the size and complexity of the company.

The business objective was to design and implement an Information Security Program to reasonably protect the security, privacy, confidentiality, and integrity of nonpublic consumer information, as contemplated by the Order. The Security Team selected the ISO/IEC 27002:2005 framework for the comprehensive information security program, as described below. Considering each risk identified in the framework standard, a determination was made as to which controls in the framework would apply to the Twitter environment, in the context of protection of nonpublic consumer information. An implementation of controls was selected, where appropriate, for managing the identified material risks.

Data Classification

(b)(4)

PwC Assessment Overview

PwC Assessor Qualifications

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

As one of the "Big 4" public accounting firms, 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") and by state societies of CPAs, state boards of accountancy, the Securities and Exchange Commission ("SEC"), and the Public Company Accounting Oversight Board ("PCAOB"). 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 CPAs who are 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 by CPAs consistently follow specific General Standards, Standards of Fieldwork, and Reporting Standards.

The following individuals from PwC led the Assessment:

- Carolyn Holcomb - Engagement Partner - Carolyn served as the lead engagement partner for the project. Carolyn is a Certified Public Accountant (CPA), Certified Information Systems Auditor (CISA), and Certified Information Privacy Professional (CIPP).
- Toby Spry - Director - Toby served as the co-lead engagement director and subject matter specialist for the project. Toby is a Certified Information Systems Auditor (CISA), Certified Information Privacy Professional (CIPP), and is certified in Risk and Information Systems Controls (CRISC).
- Lorraine Wilson - Director - Lorraine served as the co-lead engagement director for the project. Lorraine is a Chartered Accountant (CA) and Certified Information Systems Auditor (CISA).
- Chandagwinyira Mafuka - Manager - Chanda served as the lead engagement manager and led the fieldwork for the engagement. Chanda is a Certified Information Systems Auditor (CISA).

Reporting Standard

"Assurance" is a term defined by the International Framework for Assurance Engagements issued by the International Auditing and Assurance Standards Board ("IAASB") to mean "an engagement in which a practitioner expresses a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the outcome of the evaluation or measurement of a subject matter against criteria." In other words, assurance that A (the subject matter) is presented in accordance with B (the criteria) (for example, A = the Twitter Information Security Program is presented in accordance with B = ISO/IEC 27002:2005). The ability to perform an assurance engagement depends significantly on the appropriateness of A and the suitability of B as a measurement tool.

Assurance involves the testing of processes, systems, and data, as appropriate, and then assessing the findings in order to support an assurance conclusion, whether reasonable ("in our opinion, A is presented fairly, in all material respects, with B") or limited ("nothing came to our attention to indicate that A is not presented in accordance with B").

An attestation "examination" is similar to an audit, as it results in positive assurance (i.e., a "presents fairly, in all material respects" opinion) over the subject matter. The engagement is performed in accordance with Attestation Standards ("ATs") established by the AICPA or the PCAOB.

In order to accept an assurance engagement, AT 101 states that a practitioner must do the following, which PwC did in this engagement:

- Have adequate technical training and proficiency to perform the attestation engagement;
- Have adequate knowledge of the subject matter;
- Have reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users;
- Maintain independence in mental attitude in all matters relating to the engagement; and
- Exercise due professional care in planning and performance of the engagement and the preparation of the report.

As described in AT 101.24, criteria are the standards or benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter.

Suitable criteria must be objective, measurable, complete, and relevant. This means they should be free from bias and sufficiently complete so that any relevant factors omitted would not alter a conclusion about the subject matter. They also should permit reasonably consistent estimation or measurement of the subject matter from one company to another. This generally means that the criteria cannot be so subjective or vague that they are not capable of providing a reasonable basis for a meaningful conclusion.

Criteria may be external to the organization or developed internally, but must be readily available to the intended users of the assurance report. In most cases, there is no single authoritative "GAAP" as in financial statement assurance; therefore, the client needs to look to relevant regulations or frameworks, accepted industry standards, or its own internal policies and procedures when developing the criteria. These sources generally must be supplemented by company specific criteria, such as management definitions, policies, and methodologies. It is critical to have clearly articulated and understood definitions.

Independence

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

As you are aware, PwC provides various other services to the Company, including financial audit. As indicated, none of these services impair our independence for purposes of this AT101 engagement.

Assessment Approach

PwC performed the assessment in accordance with AICPA Attestation Standards Section 101, AT101 Engagements. The procedures performed by PwC were designed to:

- Assess the applicability of the framework selected by the Company to address the Company's obligations within the Consent Decree;
- Assess whether the Company addressed the relevant sections of the framework selected;
- Assess the design effectiveness of the control activities implemented by the Company to address the relevant sections of the framework; and
- Assess the operating effectiveness of the implemented control activities for the 180 days ended September 12, 2011.

PwC designed and performed procedures to evaluate the design and operating effectiveness of the control activities implemented by Twitter for the 180 day period ended September 12, 2011. Our test procedures included, where appropriate, selecting samples from throughout the period and performing a combination of inquiry, observation, and/or inspection/examination procedures to evaluate the effectiveness of the Twitter control activities documented on pages 25-73 of this document. Over the course of the 180 day assessment period, PwC performed three rounds of on-site testing procedures that included interviewing individuals from Security, Legal, IT, Operations, HR, Engineering, Networking, Trust & Safety, and Facilities. Additionally, PwC reviewed over 1,000 individual artifacts that were collected from over 100 Twitter employees across the company. Refer below for a description of the test procedures utilized by PwC to assess the design and effectiveness of Twitter's information security controls.

Inquiry: To understand the design of the safeguards implemented and how they operate to meet or exceed the protections required by Paragraph II of the order, PwC had discussions with Twitter personnel from the Security, Legal, IT, Operations, HR, Engineering, Networking, Trust & Safety, and Facilities departments. The inquiry procedures included asking the Twitter personnel about the controls, policies and procedures, systems and applications, roles and responsibilities, and the process of selecting and retaining service providers. To validate the information obtained in the discussions, PwC performed corroborative inquiry procedures with multiple individuals and, using the testing techniques below, obtained additional evidence to validate the responses.

(b)(4)

(b)(4)

Observation: PwC utilized the observation testing method to validate the design and operating effectiveness of system based controls (e.g., password settings, VPN settings, encryption settings, etc.) and physical controls (e.g., badge access card readers, locked cabinets, security cameras, etc.). In areas where Twitter has implemented system based controls or safeguards that meet or exceed the protections required by Paragraph II of the order, the PwC team met with relevant Twitter personnel and observed how the system based control is designed and how it functions.

For physical controls, the PwC team visited in-scope office and data center locations to observe the physical security controls.

(b)(4)

Examination or inspection of evidence: PwC used the examination or inspection test approach to validate the operating effectiveness of manual controls and to evaluate the sufficiency of policies and procedures implemented to address Paragraph II of the Order. PwC inspected over one thousand artifacts and documents. These included documentation of the company's policies and procedures, risk assessment, security training and awareness programs, and evidence of the design and operation effectiveness of the controls or safeguards implemented (e.g., system/product development and maintenance documentation, training evidence, system audit logs, asset management tracking logs, system administrator access lists, user authorization access forms, security legal contracts, third-party vendor audits, etc.). The nature of the evidence examined varied from control to control and, where needed, other procedures like observation and inquiry were utilized to confirm the results of the examination procedures.

(b)(4)

Paragraph III Parts A, B , C and D of the Order

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

Twitter selected the ISO/IEC 27002:2005 standard, which is a widely adopted information security standard published by the International Organization for Standardization ("ISO") and the International Electrotechnical Commission ("IEC") used by companies of all sizes and complexities to guide the initiation, implementation, maintenance, and improvement of information security programs, as the framework on which it based its Information Security Program.

Following are descriptions of the Administrative, Technical, and Physical safeguards that Twitter has in place. These safeguards are described in further detail on pages 25-73.

I. Administrative Safeguards

(b)(4)

(b)(4)

II. Technical Safeguards

(b)(4)

(b)(4)

III. Physical Safeguards

(b)(4)

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.

Twitter selected the ISO/IEC 27002:2005 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. We consider this to be an applicable framework to address the Company's obligations within the Order. The control clauses and control objectives from ISO/IEC 27002:2005 and the specific safeguards Twitter has implemented to address each applicable objective and clause are included on pages 25-73 of this document.

ISO/IEC 27002:2005 is a widely adopted industry standard that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization of different sizes and complexity. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains leading practices of control objectives and controls in the following areas of information security management:

- Security policy;
- Organization of information security;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development and maintenance;
- Information security incident management;
- Business continuity management; and
- Compliance.

The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to meet the requirements identified by a risk assessment, which Twitter performed to identify the applicable security risks and safeguards that needed to be implemented as part of its Information Security Program. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

As ISO/IEC 27002:2005 is a widely adopted industry standard used by companies of all sizes and complexities to guide the initiation, implementation, maintenance, and improvement of information security programs, the information security safeguards implemented by Twitter to address the applicable ISO/IEC 27002:2005 control objectives and clauses are appropriate to Twitter's size and complexity, the nature and scope of Twitter's activities, and the sensitivity of the nonpublic personal information collected from or about consumers as described above.

As described on pages 9-12, Twitter established its information security program by implementing administrative, technical, and physical safeguards to meet or exceed the protections required by Paragraph II of the Order. As described on pages 6-9, 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 Paragraph II of the Order, and our conclusions are on pages 20-21.

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

(b)(4)

(b)(4)

(b)(4)

(b)(4)

(b)(4)

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 101, AT101 Engagements. Refer to pages **20-21** below for PwC's conclusions.

pwc

Report of Independent Accountants

To the Management of Twitter, Inc.:

We have examined Management's Assertion, included in the accompanying Exhibit I, that as of and for the 180 days ended September 12, 2011 (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. ("the Company") 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; as described in Attachment A of Management's Assertion ("the Twitter Information Security Program"), based on the International Organization for Standardization ("ISO") / International Electrotechnical Commission ("IEC") Standard 27002:2005 ("ISO/IEC 27002:2005"); 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.

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting the effectiveness of the Twitter Information Security Program as described above and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

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 is protected, in all material respects, as of and for the 180 days ended September 12, 2011, based upon the Twitter Information Security Program set forth in Attachment A of Management's Assertion in Exhibit I.

The opinion we expressed in the preceding paragraph (i) certifies that we have gathered sufficient evidence supporting the effectiveness of the Twitter Information Security Program to provide the basis for our opinion as discussed above and accordingly, (ii) certifies that the Company's security program is operating with sufficient effectiveness as of and for the 180 days ended September 12, 2011 to provide reasonable assurance that the security, privacy, confidentiality, and integrity of nonpublic consumer information is protected and has so operated throughout the Reporting Period.

pwc

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 these specified parties.

PricewaterhouseCoopers LLP
San Jose, CA
February 24, 2012

Exhibit I
Management's Assertion

The management of Twitter represents that as of and for the 180 days ended September 12, 2011 ("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. ("the Company") 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, as described in Attachment A ("the Twitter Information Security Program"), based on the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) Standard 27002:2005 ("ISO/IEC 27002:2005"); and the 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.

Furthermore, the Company represents that for the Reporting Period, the administrative, technical, and physical safeguards within the Twitter Information Security Program as outlined in Attachment A are appropriate to its size and complexity, the nature and scope of its activities, and the nature and sensitivity of personal information collected from or about consumers and meet or exceed the protections required by Paragraph II of The Order.

Twitter, Inc.

By: ______________________
Alexander Macgillivray
General Counsel & Secretary

Attachment A to Management's Assertion: Twitter Information Security Program

This attachment describes the scope of the Twitter Information Security Program referenced in the Management Assertion on the previous page.

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. Twitter users follow the Tweets of other users. Twitter maintains a very high-velocity Internet service, facilitating the transmission currently of over a billion Tweets per week. Currently, there are over 200 million user accounts on Twitter. Twitter uses an internally-built software infrastructure hosted on multiple machines at several US data centers. Twitter's primary data center is in Sacramento, California.

Twitter, as a company, had only 29 employees in January 2009. At the beginning of 2011, it had approximately 350 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 an email address. The user may optionally provide a short biography, a location, or a picture. The user may also include his or her cell phone number for the delivery of SMS messages. Most of the above information is listed publicly on the Twitter service, including the name, username, biography, location, and picture.

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 one of the user's followers. The Direct Message is not viewable by other users.

Twitter has only one 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 performed a risk assessment, as described below, using the ISO/IEC 27002:2005 framework.

Risk Assessment Process

The Security Team, in consultation with the Legal Team, met with Engineering, Trust & Safety, HR, Finance, Facilities, and IT team leads at Twitter to conduct a risk assessment of information security practices at Twitter. The objective of the risk assessment was to identify material risks, both internal and external, that could result in the compromise of nonpublic consumer information. After identifying all data types that might constitute nonpublic consumer information, the teams conducted an inventory of the information systems and physical locations at Twitter where the identified data types may reside. The teams made a determination of the material risks, taking into account the nature and scope of Twitter's activities, the sensitivities of the nonpublic information collected, the size of the service, the number of registered users, and the size and complexity of the company.

The business objective was to design and implement an Information Security Program to reasonably protect the security, privacy, confidentiality, and integrity of nonpublic consumer information, as contemplated by the Order. The Security Team selected the ISO/IEC 27002:2005 framework for the comprehensive information security program, as described below. Considering each risk identified in the framework standard, a determination was made as to which controls in the framework would apply to the Twitter environment, in the context of protection of nonpublic consumer information. An implementation of controls was selected, where appropriate, for managing the identified material risks.

Data Classification

(b)(4)

Framework

Twitter selected the ISO/IEC 27002:2005 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. We consider this to be an applicable framework to address the Company's obligations within the Order. The control clauses and control objectives from ISO/IEC 27002:2005 and the specific safeguards Twitter has implemented to address each applicable objective and clause are included on pages 26-73 of this document.

ISO/IEC 27002:2005 is a widely adopted industry standard that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization of different sizes and complexity. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains leading practices of control objectives and controls in the following areas of information security management:

- Security policy;
- Organization of information security;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development and maintenance;
- Information security incident management;
- Business continuity management; and
- Compliance.

The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to meet the requirements identified by a risk assessment, which Twitter performed to identify the applicable security risks and safeguards that needed to be implemented as part of its Information Security Program. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

As ISO/IEC 27002:2005 is a widely adopted industry standard used by company's of all sizes and complexities to guide the initiation, implementation, maintenance, and improvement of information security programs, the information security safeguards implemented by Twitter to address the applicable ISO/IEC 27002:2005 control objectives and clauses are appropriate to Twitter's size and complexity, the nature and scope of Twitter's activities, and the sensitivity of the nonpublic personal information collected from or about consumers as described above.

I. The Twitter Information Security Program is based on the following control activities of ISO/IEC 27002:2005:

(b)(4)

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
[redacted]			

(b)(4)

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of

(b)(4)

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO

ISO Control Activity

(b)(4)

(b)(4)

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)		(b)(4)	
		perations	

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			
		(b)(4)	

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
	system.		

(b)(4)

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard

(b)(4)

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			
			[redacted]

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			
			l
			l
			l
			l

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			
			[redacted]
			[redacted]

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			[redacted]

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard

(b)(4)

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard

(b)(4)

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			
			[redacted]

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard

(b)(4)

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
(b)(4)			

II. Third-Party Developer Access to the Twitter API

An Application Programming Interface ("API") is a defined way for a program to accomplish a task, usually by retrieving or modifying data. Twitter provides an API method for just about every feature visible on the Twitter website, including the DM feature. Third-party programmers can use the Twitter API to make applications and websites that interact with Twitter. Their programs talk to the Twitter API over HTTP, the same protocol used by browsers to visit and interact with web pages. The Twitter API includes a REST API, a Streaming API, and a Search API. For the Search API, no authentication is required since the information provided by the Search API is publicly available. For the REST API and the Streaming API, an Application Permission Model is used to control access to DMs.

In order for a developer to create an application that can access information such as a user's DMs, the developer must:

- agree to the Twitter Terms of Service (https://twitter.com/tos);
- agree to the Developer Rules of the Road (https://dev.twitter.com/terms/api-terms);
- obtain a consumer key; and
- obtain a consumer secret.

The developer must specifically agree to the Twitter Terms of Service in order to obtain an account. Once logged into their account, the developer must specifically agree to the Developer Rules of the Road in order to obtain a consumer key and a consumer secret generated by Twitter. Notably, it is a principle in the Developer Rules of the Road to "[r]espect user privacy" and that Twitter may immediately suspend a developer's credentials including their consumer key and consumer secret for any violations of the Rules.

API developer users accept the Twitter API Terms of Service prior to accessing the Twitter systems through the developer API. (Twitter Control 11.2.1.2)

(b)(4)

III. The Company did not include Tweetdeck, AdGrok, Back Type, or BagCheck in the scope of the assertion.

pwc

February 24, 2012

Mr. Alexander Macgillivray
General Counsel & Secretary, Twitter
795 Folsom Street, Suite 600
San Francisco, CA 94103

Dear Mr. Macgillivray:

PricewaterhouseCoopers ("PwC" or "we" or "our" or "Assessor") is writing this letter in response to the Federal Trade Commission's ("FTC") letter to Twitter, Inc. ("Twitter" or "the Company") from Mr. Waller dated February 9, 2012 titled "re: In the Matter of Twitter, Inc., FTC Docket No. C-4316." The FTC has commented that the Assessment does not address Parts A, B, and C of Paragraph III of the Commission's Decision and Order served on March 16, 2011 Assessment ("Assessment"). In response, in the following pages, we more thoroughly address Parts A, B, and C of Paragraph III.

Should you have any questions or comments related to the procedures performed by PwC as part of our Assessment of Twitter's Information Security Program, please contact Carolyn Holcomb at (678) 419-1696, via e-mail at carolyn.c.holcomb@us.pwc.com, or physical mail at 10 10th St. NW, Suite 1400, Atlanta, GA 30309.

Sincerely,

Carolyn C. Holcomb

Executive Summary

Executive Summary

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. Twitter users follow the Tweets of other users. Twitter maintains a very high-velocity Internet service, facilitating the transmission currently of over a billion Tweets per week. Currently, there are over 200 million user accounts on Twitter. Twitter uses an internally-built software infrastructure hosted on multiple machines at several US data centers. Twitter's primary data center is in Sacramento, California.

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

Paragraph 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.

Paragraph 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 the initial assessment.

As described on pages 3-4, Twitter established its information security program by implementing administrative, technical, and physical safeguards to meet or exceed the protections required by Paragraph II of the Order. As described on pages 6-9, 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 Paragraph II of the Order, and our conclusions are on pages 20-21.

pwc

Twitter Information Security Program & Assessment 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. Twitter users follow the Tweets of other users. Twitter maintains a very high-velocity Internet service, facilitating the transmission currently of over a billion Tweets per week. Currently, there are over 200 million user accounts on Twitter. Twitter uses an internally-built software infrastructure hosted on multiple machines at several US data centers. Twitter's primary data center is in Sacramento, California.

Twitter, as a company, had only 29 employees in January 2009. At the beginning of 2011, it had approximately 350 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 an email address. The user may optionally provide a short biography, a location, or a picture. The user may also include his or her cell phone number for the delivery of SMS messages. Most of the above information is listed publicly on the Twitter service, including the name, username, biography, location, and picture.

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 one of the user's followers. The Direct Message is not viewable by other users.

Twitter Information Security Program Scope

Twitter has only one 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 performed a risk assessment, as described below, using the ISO/IEC 27002:2005 framework.

Risk Assessment Process

The Security Team, in consultation with the Legal Team, met with Engineering, Trust & Safety, HR, Finance, Facilities, and IT team leads at Twitter to conduct a risk assessment of information security practices at Twitter. The objective of the risk assessment was to identify material risks, both internal and external, that could result in the compromise of nonpublic consumer information. After identifying all data types that might constitute nonpublic consumer information, the teams conducted an inventory of the information systems and physical locations at Twitter where the identified data types may reside. The teams made a determination of the material risks, taking into account the nature and scope of Twitter's activities, the sensitivities of the nonpublic information collected, the size of the service, the number of registered users, and the size and complexity of the company.

The business objective was to design and implement an Information Security Program to reasonably protect the security, privacy, confidentiality, and integrity of nonpublic consumer information, as contemplated by the Order. The Security Team selected the ISO/IEC 27002:2005 framework for the comprehensive information security program, as described below. Considering each risk identified in the framework standard, a determination was made as to which controls in the framework would apply to the Twitter environment, in the context of protection of nonpublic consumer information. An implementation of controls was selected, where appropriate, for managing the identified material risks.

Data Classification

As part of the Twitter risk assessment, the following data types on Twitter information systems were determined as being within the scope of the order: a user's email address, mobile telephone number (if provided), a user's Direct Messages (DMs), a user's Protected Tweets, and other identifiers (such as IP address) where the information is nonpublic and individually-identifiable and associated with a user. Also included within the scope of the order was nonpublic, individually-identifiable information of employees, including their home address, social security number, birthdate, and other nonpublic individually-identifiable information, which may be found in the employee's personnel records.

PwC Assessment Overview

PwC Assessor Qualifications

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

As one of the "Big 4" public accounting firms, 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") and by state societies of CPAs, state boards of accountancy, the Securities and Exchange Commission ("SEC"), and the Public Company Accounting Oversight Board ("PCAOB"). 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 CPAs who are 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 by CPAs consistently follow specific General Standards, Standards of Fieldwork, and Reporting Standards.

The following individuals from PwC led the Assessment:

- Carolyn Holcomb - Engagement Partner - Carolyn served as the lead engagement partner for the project. Carolyn is a Certified Public Accountant (CPA), Certified Information Systems Auditor (CISA), and Certified Information Privacy Professional (CIPP).
- Toby Spry - Director - Toby served as the co-lead engagement director and subject matter specialist for the project. Toby is a Certified Information Systems Auditor (CISA), Certified Information Privacy Professional (CIPP), and is certified in Risk and Information Systems Controls (CRISC).
- Lorraine Wilson - Director - Lorraine served as the co-lead engagement director for the project. Lorraine is a Chartered Accountant (CA) and Certified Information Systems Auditor (CISA).
- Chandagwinyira Mafuka - Manager - Chanda served as the lead engagement manager and led the fieldwork for the engagement. Chanda is a Certified Information Systems Auditor (CISA).

<u>Reporting Standard</u>

"Assurance" is a term defined by the International Framework for Assurance Engagements issued by the International Auditing and Assurance Standards Board ("IAASB") to mean "an engagement in which a practitioner expresses a conclusion designed to enhance the degree of confidence of the intended users other than the responsible party about the outcome of the evaluation or measurement of a subject matter against criteria." In other words, assurance that A (the subject matter) is presented in accordance with B (the criteria) (for example, A = the Twitter Information Security Program is presented in accordance with B = ISO/IEC 27002:2005). The ability to perform an assurance engagement depends significantly on the appropriateness of A and the suitability of B as a measurement tool.

Assurance involves the testing of processes, systems, and data, as appropriate, and then assessing the findings in order to support an assurance conclusion, whether reasonable ("in our opinion, A is presented fairly, in all material respects, with B") or limited ("nothing came to our attention to indicate that A is not presented in accordance with B").

An attestation "examination" is similar to an audit, as it results in positive assurance (i.e., a "presents fairly, in all material respects" opinion) over the subject matter. The engagement is performed in accordance with Attestation Standards ("ATs") established by the AICPA or the PCAOB.

In order to accept an assurance engagement, AT 101 states that a practitioner must do the following, which PwC did in this engagement:

- Have adequate technical training and proficiency to perform the attestation engagement;
- Have adequate knowledge of the subject matter;
- Have reason to believe that the subject matter is capable of evaluation against criteria that are suitable and available to users;
- Maintain independence in mental attitude in all matters relating to the engagement; and
- Exercise due professional care in planning and performance of the engagement and the preparation of the report.

As described in AT 101.24, criteria are the standards or benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter.

Suitable criteria must be objective, measurable, complete, and relevant. This means they should be free from bias and sufficiently complete so that any relevant factors omitted would not alter a conclusion about the subject matter. They also should permit reasonably consistent estimation or measurement of the subject matter from one company to another. This generally means that the criteria cannot be so subjective or vague that they are not capable of providing a reasonable basis for a meaningful conclusion.

Criteria may be external to the organization or developed internally, but must be readily available to the intended users of the assurance report. In most cases, there is no single authoritative "GAAP" as in financial statement assurance; therefore, the client needs to look to relevant regulations or frameworks, accepted industry standards, or its own internal policies and procedures when developing the criteria. These sources generally must be supplemented by company specific criteria, such as management definitions, policies, and methodologies. It is critical to have clearly articulated and understood definitions.

Independence

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

As you are aware, PwC provides various other services to the Company, including financial audit. As indicated, none of these services impair our independence for purposes of this AT101 engagement.

Assessment Approach

PwC performed the assessment in accordance with AICPA Attestation Standards Section 101, AT101 Engagements. The procedures performed by PwC were designed to:

- Assess the applicability of the framework selected by the Company to address the Company's obligations within the Consent Decree;
- Assess whether the Company addressed the relevant sections of the framework selected;
- Assess the design effectiveness of the control activities implemented by the Company to address the relevant sections of the framework; and
- Assess the operating effectiveness of the implemented control activities for the 180 days ended September 12, 2011.

PwC designed and performed procedures to evaluate the design and operating effectiveness of the control activities implemented by Twitter for the 180 day period ended September 12, 2011. Our test procedures included, where appropriate, selecting samples from throughout the period and performing a combination of inquiry, observation, and/or inspection/examination procedures to evaluate the effectiveness of the Twitter control activities documented on pages 25-73 of this document. Over the course of the 180 day assessment period, PwC performed three rounds of on-site testing procedures that included interviewing individuals from Security, Legal, IT, Operations, HR, Engineering, Networking, Trust & Safety, and Facilities. Additionally, PwC reviewed over 1,000 individual artifacts that were collected from over 100 Twitter employees across the company. Refer below for a description of the test procedures utilized by PwC to assess the design and effectiveness of Twitter's information security controls.

Inquiry: To understand the design of the safeguards implemented and how they operate to meet or exceed the protections required by Paragraph II of the order, PwC had discussions with Twitter personnel from the Security, Legal, IT, Operations, HR, Engineering, Networking, Trust & Safety, and Facilities departments. The inquiry procedures included asking the Twitter personnel about the controls, policies and procedures, systems and applications, roles and responsibilities, and the process of selecting and retaining service providers. To validate the information obtained in the discussions, PwC performed corroborative inquiry procedures with multiple individuals and, using the testing techniques below, obtained additional evidence to validate the responses.

For example, Twitter's information security program contains control 6.1.1, which states: "Twitter has appointed a Security Manager to lead the security team and to oversee Twitter's Information Security Program. This individual is responsible for leading the Security Committee, on-boarding security training, updating and communicating policy changes, and enforcing the company's security policy. The Security Manager reports to the VP of Engineering."

In order to test this control, PwC inquired of Twitter's Legal Counsel, Compliance Project Manager, and Security Manager to determine that Twitter has appointed the Security Manager to lead the security team and oversee Twitter's Information Security Program, including responsibilities for leading the Security Committee, on-boarding security training, updating and communicating policy changes, and enforcing the company's security policy. Additionally, PwC inspected copies of the Security Committee meetings minutes confirming attendees and that the Security Manager leads the meetings and is responsible for on-boarding security training, updating and communicating policy changes, and enforcing security policy. PwC inspected an organizational chart showing that the Security Manager is responsible for the Twitter Security Team and reports directly to the VP of Engineering. PwC inspected the Employee Security Handbook ("ESH") to determine that the Security Manager represents the Security Team at all Security Committee Meetings and that the ESH included language indicating that the Security Manager and Security Team are responsible for managing overall information security as well as conducting security reviews of different systems within Twitter.

Observation: PwC utilized the observation testing method to validate the design and operating effectiveness of system based controls (e.g., password settings, VPN settings, encryption settings, etc.) and physical controls (e.g., badge access card readers, locked cabinets, security cameras, etc.). In areas where Twitter has implemented system based controls or safeguards that meet or exceed the protections required by Paragraph II of the order, the PwC team met with relevant Twitter personnel and observed how the system based control is designed and how it functions.

For physical controls, the PwC team visited in-scope office and data center locations to observe the physical security controls.

For example, Twitter's information security program contains Twitter Control 11.5.2, which states: "Each user is assigned a unique ID when accessing and performing administration activities on information systems."

In order to test this control, PwC inquired of the Twitter Compliance Project Manager to determine that admin activities are performed via SSH access, and that for a user to have an SSH key, they must have a respective LDAP account. PwC also observed as the Compliance Project Manager performed an export of all LDAP accounts from Apache Directory Studio. In order to determine that a unique user ID will be used for each LDAP account, attempted to filter the list for duplicate records and determined that no duplicates exist in the list of LDAP accounts and verified that no generic shared accounts exist.

Additionally, PwC observed as an authorized Twitter admin demonstrated the use of SSH access to production systems. Per inquiry with the Twitter admin, the use of SSH in this user's role would allow view or update access to log files (e.g., to tailor a log file for an error). PwC observed as the Twitter admin executed the appropriate command to successfully access the log file with SSH access to production. PwC then observed the Compliance Project Manager attempt to access the same log file as the Twitter admin by executing the same command without SSH access to production and determined that the Compliance Project Manager was unable to access the log file as they did not have SSH access to production.

Finally, PwC observed as the Compliance Project Manager attempted to login using LDAP authentication without a username and determined that an error was generated.

Examination or inspection of evidence: PwC used the examination or inspection test approach to validate the operating effectiveness of manual controls and to evaluate the sufficiency of policies and procedures implemented to address Paragraph II of the Order. PwC inspected over one thousand artifacts and documents. These included documentation of the company's policies and procedures, risk assessment, security training and awareness programs, and evidence of the design and operation effectiveness of the controls or safeguards implemented (e.g., system/product development and maintenance documentation, training evidence, system audit logs, asset management tracking logs, system administrator access lists, user authorization access forms, security legal contracts, third-party vendor audits, etc.). The nature of the evidence examined varied from control to control and, where needed, other procedures like observation and inquiry were utilized to confirm the results of the examination procedures.

For example, Twitter's information security program contains control 12.1.1, which states: "Project design documentation (e.g., the Technical Design Review) for SDLC projects includes, as appropriate, security requirements and input from the Security Team."

In order to test this control, PwC inspected a copy of the Software Development Lifecycle ("SDLC") policy to determine that Twitter has a formal SDLC process and policy in place that adheres to the description of the Twitter Control Activity. PwC then obtained a listing of SDLC projects that were implemented during the assessment period to determine that there was a population of twenty-eight projects. For all twenty-eight projects, PwC obtained and inspected the Technical Design Review document to determine that consideration of security requirements and input from the Security Team was appropriately considered and documented.

Paragraph III Parts A, B , C and D of the Order

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

Twitter selected the ISO/IEC 27002:2005 standard, which is a widely adopted information security standard published by the International Organization for Standardization ("ISO") and the International Electrotechnical Commission ("IEC") used by companies of all sizes and complexities to guide the initiation, implementation, maintenance, and improvement of information security programs, as the framework on which it based its Information Security Program.

Following are descriptions of the Administrative, Technical, and Physical safeguards that Twitter has in place. These safeguards are described in further detail on pages 25-73.

1. Administrative Safeguards

There is a Security Committee at Twitter that comprises representatives from the Security, Engineering, HR, and Legal teams. The Security Committee is tasked with management and review of the Information Security Program. The Security Committee meets quarterly. (Twitter Control 6.1.2) The Security Committee reviews the Information Security Program policies on an annual basis. A risk assessment is conducted by the Security Committee, and the annual review is documented. (Twitter Control 5.1.2) Twitter's Information Security Program policies are centralized in the Employee Security Handbook. The Security Manager and the Security Committee approves the contents of the Handbook. Policies are communicated via the Wiki site and new hire training. (Twitter Control 5.1.1)

Twitter has appointed a Security Manager to lead the security team and to oversee Twitter's Information Security Program. This individual is responsible for leading the Security Committee, on-boarding security training, updating and communicating policy changes, and enforcing the company's security policy. The Security Manager reports to the VP of Engineering. (Twitter Control 6.1.1)

Twitter has a documented policy related to the classification and handling of nonpublic consumer information. That policy is reviewed and updated during the annual review by the Security Committee. (Twitter Controls 7.2.1 and 7.2.2) User access, termination, and modification is granted based on job responsibility as is documented in a ticket. (Twitter Control 11.6.1.2)

HR performs a background check on all new employees, verifying education and prior employment, as well as checking criminal records. (Twitter Control 8.1.2) Employees must adhere to the policies outlined in the Employee Security Handbook and are otherwise subject to disciplinary action. (Twitter Control 8.2.3)

Upon on-boarding, employees are assigned a laptop, pre-configured with monitoring software that reports on and enforces key security settings. (Twitter Control 7.1.1.1) IT maintains an inventory of all laptops, assigned and unassigned, ensuring that all assigned laptops are accounted for at least every 14 days and unassigned laptops are accounted for quarterly. (Twitter Control 7.1.1.2) Upon off-boarding, HR initiates a process to collect assets and revoke access, which is recorded in each employee's off-boarding checklist. (Twitter Controls 7.1.1.3 and 8.3.2)

The Security Team performs comprehensive security reviews of third parties that enter a relationship with Twitter that may grant them access to sensitive data. (Twitter Controls 6.2.1) The Security Team reviews appropriate reports on an annual basis to ensure the security profile of the third-party continues to meet requirements. The Security Committee considers the status of these reviews and relationships as part of its annual risk assessment. (Twitter Control 10.2.1.1)

System owners review logical access control lists quarterly to ensure only authorized personnel are granted access to production systems. (Twitter Control 11.2.4) Twitter applies a combination of policy, configuration and training to ensure that employee passwords are sufficiently complex, changed with an appropriate frequency, and securely distributed. (Twitter Controls 11.2.3, 11.3.1)

Twitter has a formal incident management process in place, detailing personnel responsibilities and incident follow-up. (Twitter Controls 13.2.1, 13.2.2)

The Security Team participates in design and readiness review for all security-sensitive software development projects to ensure security requirements are included for all Twitter systems. (Twitter Control 12.1.1) Similarly, the Legal team participates in all new product releases to review compliance with statutory, regulatory and contractual requirements. (Twitter Control 15.1.1)

II. Technical Safeguards

Twitter uses an internally-built software infrastructure hosted on multiple machines at several US data centers. Twitter's primary data center is in Sacramento, California.

The Operations Team uses a server management platform to monitor and update operating systems on servers and ensure that they are a secure version. (Twitter Control 12.6.1.2) All production systems, including the change management system and server management platform, are access controlled. (Twitter Control 10.1.3.2) Production system logs are processed automatically and the information presented to operations personnel through event-monitoring dashboards. (Twitter Control 10.10.2) There is ongoing monitoring of server activity to detect malicious software. (Twitter Control 10.4.1.2) Twitter utilizes staging servers to separate development and staging environments from the production environment. (Twitter Control 11.4.5.2)

Twitter has implemented network security encryption, firewalls, and VPN protocols to protect the network from threats and inappropriate access. (Twitter Control 10.6.1.1) The Network Operations Team configures and monitors the network security in the data centers. The team reviews the security configurations on at least a quarterly basis. (Twitter Control 10.6.1.2) The corporate network is separated from the data center networks to secure critical production information. (Twitter Control 11.4.5.3) Twitter uses a virtual private network ("VPN") to authenticate remote users. Users have to be part of the VPN group to gain access through the VPN. (Twitter Control 11.4.2.1) VPN sessions are configured to timeout after a period of inactivity, and VPN sessions have a maximum session length. (Twitter Controls 11.5.5, 11.5.6)

All production code is checked-in to a source code repository system which maintains version history and change logs for all code files. Check-in privileges are restricted to authorized users (Twitter Control 12.4.3) Production system changes are documented in the Review Board system, capturing evidence of change approval. (Twitter Control 12.4.1) Software source code changes are documented in a Review Board ticket, capturing evidence of testing and approval. (Twitter Control 12.5.1)

The Trust & Safety group monitors and responds to abuse issues using an admin system. Modifications to user data performed using the admin system are logged. Admin logs specify operator and timestamp activities. (Twitter Control 10.10.4)

An Application Programming Interface ("API") is a defined way for a program to accomplish a task, usually by retrieving or modifying data. Twitter provides an API method for most features visible on the Twitter website, including the DM feature. Third-party programmers can use the Twitter API to make applications and websites that interact with Twitter. Their programs talk to the Twitter API over HTTP, the same protocol used by browsers to visit and interact with web pages. The Twitter API includes a REST API, a Streaming API, and a Search API. For the Search API, no authentication is required since the information provided by the Search API is publicly available. For the REST API and the Streaming API, an Application Permission Model is used to control access to DMs.

In order for a developer to create an application that can access information such as a user's DMs, the developer must:

- agree to the Twitter Terms of Service (https://twitter.com/tos)
- agree to the Developer Rules of the Road (https://dev.twitter.com/terms/api-terms)
- obtain a consumer key
- obtain a consumer secret

The developer must specifically agree to the Twitter Terms of Service in order to obtain an account. Once logged into their account, the developer must specifically agree to the Developer Rules of the Road in order to obtain a consumer key and a consumer secret generated by Twitter. Notably, it is a principle in the Developer Rules of the Road to "[r]espect user privacy" and that Twitter may immediately suspend a developer's credentials including their consumer key and consumer secret for any violations of the Rules.

Twitter utilizes the OAuth protocol to control access to user data by third-party developers. The API documentation details Twitter's security implementation requirements. Any API changes that could affect security of information protected by the API are reviewed for approval by the Security Team, and by the Legal Team if they also impact existing policies, agreements, or terms. (Twitter Control 10.2.1.2) Twitter monitors operational activities to identify large scale API inappropriate activity. Inappropriate activity will result in API shutdown. (Twitter Control 10.2.2.1)

III. Physical Safeguards

Twitter's corporate headquarters has the proper physical and environmental protections in place to protect against damage from natural or man-made disasters, including, but not limited to: access badge readers throughout the building and in elevators, 24-hour on-site security, video surveillance systems, alarm systems, sprinkler systems, etc. (Twitter Control 9.1.4.1)

Physical security controls have been designed and applied at data centers such as the Sacramento facility by the third-party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third-party compliance with security requirements. Site operations personnel are responsible for maintaining the equipment in the data centers, as documented by Site Operations procedures. (Twitter Controls 9.1.4.2-4)

An electronic access badge is required to enter corporate offices and data centers. (Twitter Controls 9.1.1-2)

For a full list of Twitter's administrative, technical, and physical controls implemented, maintained and evaluated by PwC as part of the Security Assessment, refer to the table on pages 25-73 of this document.

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.

Twitter selected the ISO/IEC 27002:2005 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. We consider this to be an applicable framework to address the Company's obligations within the Order. The control clauses and control objectives from ISO/IEC 27002:2005 and the specific safeguards Twitter has implemented to address each applicable objective and clause are included on pages 25-73 of this document.

ISO/IEC 27002:2005 is a widely adopted industry standard that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization of different sizes and complexity. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains leading practices of control objectives and controls in the following areas of information security management:

- Security policy;
- Organization of information security;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development and maintenance;
- Information security incident management;
- Business continuity management; and
- Compliance.

The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to meet the requirements identified by a risk assessment, which Twitter performed to identify the applicable security risks and safeguards that needed to be implemented as part of its Information Security Program. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

As ISO/IEC 27002:2005 is a widely adopted industry standard used by companies of all sizes and complexities to guide the initiation, implementation, maintenance, and improvement of information security programs, the information security safeguards implemented by Twitter to address the applicable ISO/IEC 27002:2005 control objectives and clauses are appropriate to Twitter's size and complexity, the nature and scope of Twitter's activities, and the sensitivity of the nonpublic personal information collected from or about consumers as described above.

As described on pages 9-12, Twitter established its information security program by implementing administrative, technical, and physical safeguards to meet or exceed the protections required by Paragraph II of the Order. As described on pages 6-9, 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 Paragraph II of the Order, and our conclusions are on pages 20-21.

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

As summarized in the Twitter Control Activities on pages 26-73 Twitter has implemented the following protections:

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

Twitter has appointed a Security Manager to lead the security team and to oversee Twitter's Information Security Program. This individual is responsible for leading the Security Committee, on-boarding security training, updating and communicating policy changes, and enforcing the company's security policy. The Security Manager reports to the VP of Engineering. (Twitter Control 6.1.1)

Additionally, there is a Security Committee that comprises representatives from Security, Engineering, HR, and Legal. The Security Committee is tasked with management and review of the Information Security Program. The Security Committee meets quarterly. (Twitter Control 6.1.2)

As described on pages 9-12, Twitter established its information security program by implementing administrative, technical, and physical safeguards to meet or exceed the protections required by Paragraph II of the Order. As described on pages 6-9, 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 Paragraph II of the Order, and our conclusions are on pages 20-21.

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.

Risk Assessment Process
The Security Team, in consultation with the Legal Team, met with Engineering, Trust & Safety, HR, Finance, Facilities, and IT team leads at Twitter to conduct a risk assessment of information

security practices at Twitter. The objective of the risk assessment was to identify material risks, both internal and external, that could result in the compromise of nonpublic consumer information. After determining which products/services were within the scope of the order, the teams identified all data types that might constitute nonpublic consumer information and would need to be protected. The teams conducted an inventory of the information systems at Twitter where the identified data types may be stored or processed, and they identified the physical locations where the identified data types, in electronic or paper form, may reside. The teams determined which groups of employees had authorized access to the information systems and locations as well as which non-Twitter service providers may have been provided with access to the nonpublic consumer information. Then, a determination was made of the material risks, taking into account the nature and scope of Twitter's activities, the sensitivities of the nonpublic information collected, the size of the service, the number of registered users, and the size and complexity of the company. Examples of risks included unauthorized access to Twitter systems, including Twitter admin systems, unauthorized access to Twitter locations, and misuse of authorized access to Twitter systems.

The business objective was to design and implement an Information Security Program to reasonably protect the security, privacy, confidentiality, and integrity of nonpublic consumer information, as contemplated by the Order. After identification of materials risks, an initial determination was conducted of the sufficiency of existing safeguards in place to control these risks. The Security Team then selected a framework for the comprehensive information security program. Considering each risk identified in the framework standard, a determination was made as to which controls in the framework would apply to the Twitter environment, in the context of protection of nonpublic consumer information. An implementation of controls was selected, where appropriate for managing the identified material risks. Then, a determination was made as to whether there were any additional risks in the Twitter environment that would not be controlled by the relevant controls or existing safeguards.

Additionally, the Security Committee reviews the Information Security Program policies on an annual basis. A risk assessment is conducted by the Security Committee, and the annual review is documented, as specified in the Employee Security Handbook. Significant changes are communicated via email and the wiki. (Twitter Control 5.1.2)

Refer to pages 3-4 of this document for a description of Twitter's Information Security Program safeguards implemented and maintained during the period related to 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 the assessment of the sufficiency of safeguards in place to control these risks.

As described on pages 3-4, Twitter established its information security program by implementing administrative, technical, and physical safeguards to meet or exceed the protections required by Paragraph II of the Order. As described on pages 6-9, 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 Paragraph II of the Order, and our conclusions are on pages 20-21

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.

Design & Implementation of Safeguards
Based on the risks identified through the risk assessment described in B. above, Twitter designed and implemented the administrative, technical, and physical safeguards documented on pages 26-73

Regular Testing & Monitoring of Safeguards
The Security Committee performs an annual review of the overall Information Security Program. As an input to that review, the security team will select controls for testing based on a plan and will validate that the remaining untested controls are in place. (Twitter Control 15.2.2.1)

Additionally, Twitter has the following monitoring controls that align to the Monitoring Objective of the ISO/IEC 27002:2005 framework:

- User activities, exceptions, and information security events are produced and retained according to an internal data retention policy. (Twitter Control 10.10.1)

- Production system logs are processed automatically and the information presented to operations personnel through event-monitoring dashboards. (Twitter Control 10.10.2)

- Only authorized users have access to log systems. Modify access to the log systems is further restricted to a smaller set of authorized users. A quarterly review is conducted of authorized users. (Twitter Control 10.10.3)

- Modifications to user data performed using the admin system are logged. Admin logs specify operator and timestamp of activities. The Trust & Safety group monitors and responds to abuse issues. (Twitter Control 10.10.4)

As described on pages 9-12-, Twitter established its information security program by implementing administrative, technical, and physical safeguards to meet or exceed the protections required by Paragraph II of the Order. As described on pages 6-9, 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 Paragraph II of the Order, and our conclusions are on pages 20-21.

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.*

Selection of Service Providers
Legal reviews all agreements and informs Security of any that require review, including those that may access nonpublic consumer information. If the access provided to the third-party is by other than a standardized API, the Security Team performs a security review of interfaces with the third-party and the procedures used by the third-party to protect the information. (Twitter Control 10.2.1.1)

Retention of Service Providers
Physical security controls have been designed and applied at the third-party facility by the third-party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third-party compliance with security requirements. (Twitter Controls 9.1.3.2-4) Twitter obtains and reviews the data center providers' SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third-party compliance with security requirements. (Twitter Control 10.2.1.3) Twitter obtains and reviews the ADP SAS70 on an annual basis to monitor third-party compliance with security requirements surrounding sensitive employee and payroll information. (Twitter Control 10.2.1.4)

The Security Committee performs a review of third parties as part of its annual review. (Twitter Control 10.2.2.2) The security review includes obtaining and reviewing the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis. (Twitter Control 6.2.3.2)

Third-Party Developer Access to the Twitter API
An Application Programming Interface ("API") is a defined way for a program to accomplish a task, usually by retrieving or modifying data. Twitter provides an API method for just about every feature visible on the Twitter website, including the DM feature. Third-party programmers can use the Twitter API to make applications and websites that interact with Twitter. Their programs talk to the Twitter API over HTTP, the same protocol used by browsers to visit and interact with web pages. The Twitter API includes a REST API, a Streaming API, and a Search API. For the Search API, no authentication is required since the information provided by the Search API is publicly available. For the REST API and the Streaming API, an Application Permission Model is used to control access to DMs.

In order for a developer to create an application that can access information such as a user's DMs, the developer must:

- agree to the Twitter Terms of Service (https://twitter.com/tos);
- agree to the Developer Rules of the Road (https://dev.twitter.com/terms/api-terms);
- obtain a consumer key; and

- obtain a consumer secret.

The developer must specifically agree to the Twitter Terms of Service in order to obtain an account. Once logged into their account, the developer must specifically agree to the Developer Rules of the Road in order to obtain a consumer key and a consumer secret generated by Twitter. Notably, it is a principle in the Developer Rules of the Road to "[r]espect user privacy" and that Twitter may immediately suspend a developer's credentials including their consumer key and consumer secret for any violations of the Rules.

API developer users accept the Twitter API Terms of Service prior to accessing the Twitter systems through the developer API. (Twitter Control 11.2.1.2)

Twitter utilizes the OAuth protocol to control access to user data by third-party developers. The API documentation details Twitter's security implementation requirements. Any API changes that could affect security of information protected by the API are reviewed for approval by the Security Team, and by the Legal Team if they also impact existing policies, agreements, or terms. (Twitter Control 10.2.1.2) Twitter monitors operational activities to identify large scale API inappropriate activity. Inappropriate activity will result in API shutdown. (Twitter Control 10.2.2.1)

As described on pages 9-12, Twitter established its information security program by implementing administrative, technical, and physical safeguards to meet or exceed the protections required by Paragraph II of the Order. As described on pages 6-9, 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 Paragraph II of the Order, and our conclusions are on pages 20-21.

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.

Twitter's Security Committee performs an annual review of the overall Information Security Program. As an input to that review, the security team will select controls for testing based on a plan and will validate that the remaining untested controls are in place. (Twitter Control 6.1.8)

As described on pages 3-4, Twitter established its information security program by implementing administrative, technical, and physical safeguards to meet or exceed the protections required by Paragraph II of the Order. As described on pages 6-9, 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 Paragraph II of the Order, and our conclusions are on pages 20-21.

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 101, AT101 Engagements. Refer to pages **20-21** below for PwC's conclusions.

pwc

Report of Independent Accountants

To the Management of Twitter, Inc.:

We have examined Management's Assertion, included in the accompanying Exhibit I, that as of and for the 180 days ended September 12, 2011 (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. ("the Company") 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; as described in Attachment A of Management's Assertion ("the Twitter Information Security Program"), based on the International Organization for Standardization ("ISO") / International Electrotechnical Commission ("IEC") Standard 27002:2005 ("ISO/IEC 27002:2005"); 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.

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included examining, on a test basis, evidence supporting the effectiveness of the Twitter Information Security Program as described above and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

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 is protected, in all material respects, as of and for the 180 days ended September 12, 2011, based upon the Twitter Information Security Program set forth in Attachment A of Management's Assertion in Exhibit I.

The opinion we expressed in the preceding paragraph (i) certifies that we have gathered sufficient evidence supporting the effectiveness of the Twitter Information Security Program to provide the basis for our opinion as discussed above and accordingly, (ii) certifies that the Company's security program is operating with sufficient effectiveness as of and for the 180 days ended September 12, 2011 to provide reasonable assurance that the security, privacy, confidentiality, and integrity of nonpublic consumer information is protected and has so operated throughout the Reporting Period.

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 these specified parties.

PricewaterhouseCoopers LLP
San Jose, CA
February 24, 2012

Exhibit I
Management's Assertion

The management of Twitter represents that as of and for the 180 days ended September 12, 2011 ("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. ("the Company") 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, as described in Attachment A ("the Twitter Information Security Program"), based on the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) Standard 27002:2005 ("ISO/IEC 27002:2005"); and the 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.

Furthermore, the Company represents that for the Reporting Period, the administrative, technical, and physical safeguards within the Twitter Information Security Program as outlined in Attachment A are appropriate to its size and complexity, the nature and scope of its activities, and the nature and sensitivity of personal information collected from or about consumers and meet or exceed the protections required by Paragraph II of The Order.

Twitter, Inc.

By: ______________________

Alexander Macgillivray
General Counsel & Secretary

Attachment A to Management's Assertion: Twitter Information Security Program

This attachment describes the scope of the Twitter Information Security Program referenced in the Management Assertion on the previous page.

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. Twitter users follow the Tweets of other users. Twitter maintains a very high-velocity Internet service, facilitating the transmission currently of over a billion Tweets per week. Currently, there are over 200 million user accounts on Twitter. Twitter uses an internally-built software infrastructure hosted on multiple machines at several US data centers. Twitter's primary data center is in Sacramento, California.

Twitter, as a company, had only 29 employees in January 2009. At the beginning of 2011, it had approximately 350 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 an email address. The user may optionally provide a short biography, a location, or a picture. The user may also include his or her cell phone number for the delivery of SMS messages. Most of the above information is listed publicly on the Twitter service, including the name, username, biography, location, and picture.

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 one of the user's followers. The Direct Message is not viewable by other users.

Twitter has only one 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 performed a risk assessment, as described below, using the ISO/IEC 27002:2005 framework.

Risk Assessment Process

The Security Team, in consultation with the Legal Team, met with Engineering, Trust & Safety, HR, Finance, Facilities, and IT team leads at Twitter to conduct a risk assessment of information security practices at Twitter. The objective of the risk assessment was to identify material risks, both internal and external, that could result in the compromise of nonpublic consumer information. After identifying all data types that might constitute nonpublic consumer information, the teams conducted an inventory of the information systems and physical locations at Twitter where the identified data types may reside. The teams made a determination of the material risks, taking into account the nature and scope of Twitter's activities, the sensitivities of the nonpublic information collected, the size of the service, the number of registered users, and the size and complexity of the company.

The business objective was to design and implement an Information Security Program to reasonably protect the security, privacy, confidentiality, and integrity of nonpublic consumer information, as contemplated by the Order. The Security Team selected the ISO/IEC 27002:2005 framework for the comprehensive information security program, as described below. Considering each risk identified in the framework standard, a determination was made as to which controls in the framework would apply to the Twitter environment, in the context of protection of nonpublic consumer information. An implementation of controls was selected, where appropriate, for managing the identified material risks.

Data Classification

As part of the Twitter risk assessment, the following data types on Twitter information systems were determined as being within the scope of the order: a user's email address, mobile telephone number (if provided), a user's Direct Messages (DMs), a user's Protected Tweets, and other identifiers (such as IP address) where the information is nonpublic and individually-identifiable and associated with a user. Also included within the scope of the order was nonpublic, individually-identifiable information of employees, including their home address, social security number, birthdate, and other nonpublic individually-identifiable information, which may be found in the employee's personnel records.

Framework

Twitter selected the ISO/IEC 27002:2005 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. We consider this to be an applicable framework to address the Company's obligations within the Order. The control clauses and control objectives from ISO/IEC 27002:2005 and the specific safeguards Twitter has implemented to address each applicable objective and clause are included on pages 26-73 of this document.

ISO/IEC 27002:2005 is a widely adopted industry standard that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization of different sizes and complexity. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains leading practices of control objectives and controls in the following areas of information security management:

- Security policy;
- Organization of information security;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development and maintenance;
- Information security incident management;
- Business continuity management; and
- Compliance.

The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to meet the requirements identified by a risk assessment, which Twitter performed to identify the applicable security risks and safeguards that needed to be implemented as part of its Information Security Program. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

As ISO/IEC 27002:2005 is a widely adopted industry standard used by company's of all sizes and complexities to guide the initiation, implementation, maintenance, and improvement of information security programs, the information security safeguards implemented by Twitter to address the applicable ISO/IEC 27002:2005 control objectives and clauses are appropriate to Twitter's size and complexity, the nature and scope of Twitter's activities, and the sensitivity of the nonpublic personal information collected from or about consumers as described above.

I. The Twitter Information Security Program is based on the following control activities of ISO/IEC 27002:2005:

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
5.1 Information security policy Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.			
5.1.1	An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.	Twitter's Information Security Program policies are centralized in the Employee Security Handbook. The Security Manager and the Security Committee approves the contents of the Handbook. Policies are communicated via the Wiki site and new hire training. New hires initial sign-in log to confirm attendance of training and review of the Employee Security Handbook.	Administrative
5.1.2	The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	The Security Committee reviews the Information Security Program policies on an annual basis. A risk assessment is conducted by the Security Committee, and the annual review is documented, as specified in the Employee Security Handbook. Significant changes are communicated via email and the wiki.	Administrative
6.1 Internal Organization Objective: To manage information security within the organization.			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
6.1.1	Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. (Internal)	Twitter has appointed a Security Manager to lead the security team and to oversee Twitter's Information Security Program. This individual is responsible for leading the Security Committee, on-boarding security training, updating and communicating policy changes, and enforcing the company's security policy. The Security Manager reports to the VP of Engineering.	Administrative
6.1.2	Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions. (External)	There is a Security Committee comprised of representatives from Security, Engineering, HR, and Legal. The Security Committee is tasked with management and review of the Information Security Program. The Security Committee meets quarterly.	Administrative
6.1.3	All information security responsibilities should be clearly defined.	Twitter has job descriptions and maintains them on jobvite.com. Information security responsibilities are clearly defined in the relevant job descriptions. Updates are sent to HR which updates the descriptions.	Administrative
6.1.4	A management authorization process for new information processing facilities should be defined and implemented.	6.1.4.1 The Security Manager is involved in the authorization of new information processing facilities that involve new physical locations prior to moving in. 6.1.4.2 Twitter has a policy that governs the use of personal or privately owned devices, systems and applications.	Administrative

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
6.1.5	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed.	Twitter has a confidentiality and non-disclosure policy that is required to be read and signed by new hires during their onboarding process. The policy is/are reviewed by HR and Legal on an annual basis.	Administrative
6.1.8	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.	The Security Committee performs an annual review of the overall Information Security Program. As an input to that review, the security team will select controls for testing based on a plan and will validate that the remaining untested controls are in place.	Administrative
6.2 External Parties Objective: To maintain the security of the organization's information and information facilities that are accessed, processed, communicated to, or managed by external parties.			
6.2.1	The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.	6.2.3.1 Twitter performs a security review of all third party agreements that includes review and approval by legal and the security team. 6.2.3.2 Additionally, Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to	Administrative

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		monitor third party compliance with security requirements.	
6.2.2	All identified security requirements should be addressed before giving customers access to the organization's information or assets.	**6.2.3.1** Twitter performs a security review of all third party agreements that includes review and approval by legal and the security team. **6.2.3.2** Additionally, Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security requirements.	Administrative
6.2.3	Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.	**6.2.3.1** Twitter performs a security review of all third party agreements that includes review and approval by legal and the security team. **6.2.3.2** Additionally, Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security requirements.	Administrative
7.1 Responsibility for assets Objective: To achieve and maintain appropriate protection of organizational assets.			

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
7.1.1	All assets should be clearly identified and an inventory of all important assets drawn up and maintained.	7.1.1.1 During on-boarding, each employee is assigned a laptop. Each laptop is tagged and clearly identified and is issued with a standard image installed which includes Casper, a laptop monitoring tool. When the laptop is first imaged, a Casper record is created. 7.1.1.2 Casper supports automated periodic inventory by checking in with a central server multiple times a day, when the laptop is on the corporate network. Weekly, IT reviews the last log on date and follows up on any laptop that has not checked in for more than 10 days to ensure all laptops are accounted for. 7.1.1.3 Twitter has an off-boarding checklist which ensures that employees and contractors return the company's assets in their possession. The checklist is completed by HR, IT and other departments, as appropriate as part of the termination process. 7.1.1.4 Data center hardware (i.e., servers) are tagged to ensure they are clearly identified and inventoried. Management performs quarterly cycle counts to ensure physical assets are still properly accounted for.	Administrative

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
7.1.2	All information and assets associated with information processing facilities should be owned by a designated part of the organization.	7.1.2.1 During on-boarding, each employee is assigned a laptop. Each laptop is tagged and clearly identified and is issued with a standard image installed which includes Casper, a laptop monitoring tool. When the laptop is first imaged, a Casper record is created. 7.1.2.2 Casper supports automated periodic inventory by checking in with a central server multiple times a day, when the laptop is on the corporate network. Weekly, IT reviews the last log on date and follows up on any laptop that has not checked in for more than 10 days to ensure all laptops are accounted for. 7.1.2.3 Data center hardware (i.e., servers) are tagged to ensure they are clearly identified and inventoried. Management performs quarterly cycle counts to ensure physical assets are still properly accounted for.	Administrative
7.1.3	Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.	Twitter has an acceptable use policy and agreement that is signed upon employment and/or issuance of new laptop.	Administrative

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
7.2 Information classification Objective: To ensure that information receives an appropriate level of protection.			
7.2.1	Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.	7.2.1.1 Twitter has a documented policy related to the classification of sensitive information. 7.2.1.2 Twitter's Information Security Program policies are centralized in the Employee Security Handbook. The Security Manager and the Security Committee approves the contents of the Handbook. Policies are communicated via the Wiki site and new hire training. New hires initial sign-in log to confirm attendance of training and review of the Employee Security Handbook.	Administrative
7.2.2	An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization.	Twitter has a documented policy regarding handling of nonpublic consumer information. That policy is reviewed and updated during the annual review by the Security Committee.	Administrative
8.1 Prior to employment Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.			
8.1.1	Security roles and responsibilities of employees, contractors and third	Job descriptions are maintained by HR in Jobvite.com. Updates are sent to HR which	Administrative

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
	party users should be defined and documented in accordance with the organization's information security policy.	updates the descriptions. For contractors and consultants, job descriptions are specified in their contract containing a statement of work.	
8.1.2	Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.	Background checks are performed by HR and stored on Hire-Right. The background check for full-time employees includes the following: social security number, criminal record, past three employers, educational record. Where security assurances are not provided by contracting agency, a background check is performed for contractors.	Administrative
8.1.3	As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security.	Twitter requires a signed Employee Invention assignment and confidentiality agreement from employees and contractors at the time of hiring, which include Twitter's and the employee's responsibilities for information security.	Administrative
8.2 During employment Objective: To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.			
8.2.1	Management should require employees, contractors and third party users to apply security in accordance with established policies	Twitter requires employees to sign an Employee Invention Assignment and Confidentiality Agreement Form. Consultants are required to sign an	Administrative

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
	and procedures of the organization.	agreement with a privacy statement. Third party contractors are required to sign a NDA which addresses privacy.	
8.2.2	All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.	Twitter's Information Security Program policies are centralized in the Employee Security Handbook. The Security Manager and the Security Committee approves the contents of the Handbook. Policies are communicated via the Wiki site and new hire training. New hires initial sign-in log to confirm attendance of training and review of the Employee Security Handbook. Relevant security-related updates are distributed via e-mail and/or updates to the policies.	Administrative
8.2.3	There should be a formal disciplinary process for employees who have committed a security breach.	Twitter has implemented a disciplinary process for security violations in the Employee Security Handbook. In accordance with that process, any violation of the security principles or guidelines should be reported to Manager and Security Team. If discipline is warranted, refer to Operating Committee.	Administrative
8.3 Termination or change of employment Objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.			
8.3.1	Responsibilities for performing	The VP of HR and HR Business Partner are	Administrative

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
	employment termination or change of employment should be clearly defined and assigned.	responsible for employment termination and change of employment in the company. The responsibilities are defined in the off-boarding checklist.	
8.3.2	All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their employment, contract or agreement.	Twitter has an off-boarding checklist which ensures that employees and contractors return the company's assets in their possession. This checklist is completed by HR as part of the termination process.	Administrative
8.3.3	The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Upon termination, HR facilitates an email to relevant functional owners requiring them to remove access. The functional owner is required to initial the off-boarding checklist when action has been taken.	Administrative
9.1 Secure areas Objective: To prevent unauthorized physical access, damage, and interference to the organization's premises and information.			
9.1.1	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.	An electronic access badge is required to enter corporate offices and data centers. Existing controls regarding on-boarding and off-boarding also include procedures for granting and terminating badge access.	Physical
9.1.2	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	An electronic access badge is required to enter corporate offices and data centers. Existing controls regarding on-boarding and off-boarding also include procedures for	Physical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		granting and terminating badge access.	
9.1.3	Physical security for offices, rooms, and facilities should be designed and applied.	9.1.3.1 - Corporate Confidential information is stored and maintained in a locked filing room. Physical access is restricted through a key lock which is only made available to appropriate employees. 9.1.3.2 - Sacramento Physical security controls have been designed and applied at the Sacramento facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security requirements. 9.1.3.3 - San Jose Physical security controls have been designed and applied at the San Jose facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security requirements. 9.1.3.4 - Bluffdale Physical security controls have been	Physical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		designed and applied at the Bluffdale facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security requirements.	
9.1.4	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.	9.1.4.1 - Corporate Twitter's corporate headquarters has the proper physical and environmental protections in place to protect against damage from natural or man-made disasters, including, but not limited to: access badge readers throughout the building and in elevators, 24-hour on-site security, video surveillance systems, alarm systems, sprinkler systems, etc. 9.1.4.2 - Sacramento Physical security and environmental controls have been designed and applied at the Sacramento facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security and environmental requirements. 9.1.3.3 - San Jose Physical security and environmental controls	Physical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		have been designed and applied at the San Jose facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security and environmental requirements. 9.1.3.4 - Bluffdale Physical security and environmental controls have been designed and applied at the Bluffdale facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security and environmental requirements.	
9.1.5	Physical protection and guidelines for working in secure areas should be designed and applied.	Twitter has documented physical data center security procedures which are distributed to employees who work in data centers. Employees acknowledge receipt and review the procedures. The procedures are reviewed for updates on an annual basis.	Physical
9.2 Equipment security Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.			
9.2.1	Equipment should be protected to reduce the risks from environmental	9.2.1.1 - Corporate Twitter's corporate headquarters has the	Physical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
	threats and hazards, and opportunities for unauthorized access.	proper physical and environmental protections in place to protect against damage from natural or man-made disasters, including, but not limited to: access badge readers throughout the building and in elevators, 24-hour on-site security, video surveillance systems, alarm systems, sprinkler systems, etc. 9.2.1.2 - Sacramento Physical security and environmental controls have been designed and applied at the Sacramento facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security and environmental requirements. 9.2.1.3 - San Jose Physical security and environmental controls have been designed and applied at the San Jose facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security and environmental requirements. 9.2.1.4 - Bluffdale Physical security and environmental controls have been designed and applied at the	

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		Bluffdale facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security and environmental requirements.	
9.2.2	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.	9.2.2.1 - Corporate Twitter's corporate headquarters has the proper physical and environmental protections in place to protect against damage from natural or man-made disasters, including, but not limited to: access badge readers throughout the building and in elevators, 24-hour on-site security, video surveillance systems, alarm systems, sprinkler systems, etc. 9.2.2.2 - Sacramento Physical security and environmental controls have been designed and applied at the Sacramento facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security and environmental requirements. 9.2.2.3 - San Jose Physical security and environmental controls have been designed and applied at the San	Physical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		Jose facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security and environmental requirements. 9.2.2.4 - Bluffdale Physical security and environmental controls have been designed and applied at the Bluffdale facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security and environmental requirements.	
9.2.3	Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.	9.2.3.1 - Corporate Twitter's corporate headquarters has the proper physical and environmental protections in place to protect against damage from natural or man-made disasters, including, but not limited to: access badge readers throughout the building and in elevators, 24-hour on-site security, video surveillance systems, alarm systems, sprinkler systems, etc. 9.2.3.2 - Sacramento Physical security and environmental controls have been designed and applied at the	Physical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		Sacramento facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security and environmental requirements. 9.2.3.3 - San Jose Physical security and environmental controls have been designed and applied at the San Jose facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security and environmental requirements. 9.2.3.4 - Bluffdale Physical security and environmental controls have been designed and applied at the Bluffdale facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security and environmental requirements.	
9.2.4	Equipment should be correctly maintained to ensure its continued availability and integrity.	Site Operations personnel are responsible for maintaining the equipment in the data centers, as documented by Site Operations	Physical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		procedures.	
9.2.5	Security should be applied to off-site equipment taking into account the different risks of working outside the organization's premises.	9.2.5.1 - Sacramento Physical security and environmental controls have been designed and applied at the Sacramento facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security and environmental requirements. 9.2.5.2 - San Jose Physical security and environmental controls have been designed and applied at the San Jose facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security and environmental requirements. 9.2.5.3 - Bluffdale Physical security and environmental controls have been designed and applied at the Bluffdale facility by the third party data center provider. Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security	Physical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		and environmental requirements.	
9.2.6	All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.	Twitter secures or destroys all private data on laptop hardware before disposing of laptops The Site Operations Team has a process for the secure destruction of hard drives.	Physical
9.2.7	Equipment, information or software should not be taken off-site without prior authorization.	Twitter policy as defined in the Employee Security handbook requires employees to engage the security team before moving sensitive data to a non-Twitter machine or removable media.	Physical
10.1 Operational procedures and responsibilities Objective: To ensure the correct and secure operation of information processing facilities.			
10.1.1	Operating procedures should be documented, maintained, and made available to all users who need them.	Twitter maintains operating procedures on the Wiki for the Operations, Site Operations, Network Engineering, Release, and Information Technology teams.	Technical
10.1.2	Changes to information processing facilities and systems should be controlled.	10.1.2.1 All operations changes are managed according to operating procedures defined and maintained by Twitter on the Wiki. 10.1.2.2 All software source code changes are documented in a Review Board ticket,	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		capturing evidence of testing and approval. For all projects, the project team either documents that security has been considered or engages the Security Team, as documented in the Technical Design Review. Conformance to the design review is reviewed and checked in the production Readiness Review. 10.1.2.3 Changes to operating systems are tested to validate that there is no adverse impact to the in-scope applications and documented in a Jira ticket.	
10.1.3	Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	10.1.3.1 Duties are segregated between the Network, Operations Engineering and Release teams. Access to production systems is restricted to engineers or employees whose functional duties require physical or SSH access. 10.1.3.2 All production systems, including change management system and server management platform, are access-controlled. Server management platform enforces distribution of approved changes.	Technical
10.1.4	Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational	Twitter utilizes staging servers to separate development and staging environments from the production environment.	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
	system.		
10.2 Third party service delivery management Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.			
10.2.1	It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.	10.2.1.1 Legal reviews all agreements and informs Security of any that require review, including those with may access nonpublic consumer information. If the access provided to the third party is by other than a standardized API, the Security Team shall do a security review of interfaces with the third party and the procedures used by the third party to protect the information. 10.2.1.2 Twitter utilizes the OAuth protocol to control access to user data by third party developers. The API documentation details Twitter's security implementation requirements. Any API changes that could affect security of information protected by the API are reviewed for approval by the Security Team, and by the Legal Team, if they also impact existing policies, agreements or terms. 10.2.1.3 Twitter obtains and reviews the data center providers' SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		monitor third party compliance with security requirements. 10.2.1.4 Twitter obtains and reviews the ADP SAS70 on an annual basis to monitor third party compliance with security requirements surrounding sensitive employee and payroll information.	
10.2.2	The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.	10.2.2.1 Twitter monitors operational activities to identify large scale API inappropriate activity. Inappropriate activity will result in API shutdown. 10.2.2.2 The Security Committee performs a review of third parties as part of its annual review. 10.2.2.3 Twitter obtains and reviews the data center providers' SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security requirements. 10.2.2.4 Twitter obtains and reviews the ADP SAS70 on an annual basis to monitor third party compliance with security requirements surrounding sensitive employee and payroll	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		information.	
10.2.3	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.	The Security Committee examines relevant changes to third party relationships in its annual review.	Technical
10.4 Protection against malicious and mobile code Objective: To protect the integrity of software and information.			
10.4.1	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.	10.4.1.1 - Corporate Twitter has a corporate policy that governs usage of IT facilities. Introducing malicious code is not permitted. Casper is used to monitor the usage of laptops. 10.4.1.2 - Data centers Servers are managed by a change management system and a server management platform (Puppet) which enforces distribution of approved changes. There is ongoing monitoring of server activity to detect malicious software.	Technical
10.4.2	Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly	12.6.1.1 The IT Group uses Casper to monitor and update individual operating systems on laptops and ensure that they are a recent	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
	defined security policy, and unauthorized mobile code should be prevented from executing.	version, limiting code vulnerabilities. 12.6.1.2 The Ops Team uses a server management platform (Puppet) to monitor and update operating systems on servers and ensure that they are a secure version. There is a procedure in a testing environment to test patches before deployment.	
10.6 Network security management Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.			
10.6.1	Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	10.6.1.1 Twitter has implemented network security encryption, firewalls and VPN protocols to protect the network from threats and inappropriate access. 10.6.1.2 The Network Operations Team configures and monitors the network security in the data centers. The IT Team configures and monitors the network security in the corporate office network. The teams review the security configurations on at least a quarterly basis. 10.6.1.3 The corporate network is separated from the data center networks to secure critical production information.	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
10.6.2	Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	10.6.2.1 All network services agreements are reviewed by the Legal Team with the business team. Standard SMS agreements may be executed by responsible delegates without Legal Team review. 10.6.2.2 The Security Manager is involved in the authorization of new information processing facilities that involve new physical locations prior to moving in.	Technical
10.7 Media handling Objective: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.			
10.7.1	There should be procedures in place for the management of removable media.	Removable media should not be used to store nonpublic consumer information, unless approved by the Security Team in a ticket. Twitter policy is documented in the Employee Security Handbook, which is communicated, reviewed and confirmed by employees during on-boarding	Technical
10.7.2	Media and Physical Documentation should be disposed of securely and safely when no longer required, using formal procedures.	When no longer needed, sensitive documents are disposed of in official shred bins located throughout the office. Twitter's DocCage policy requires that all retained documents should be filed and stored in secured file cabinets, and, after an appropriate amount of	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		time, all documents should be disposed in official shred bins located throughout the Twitter facilities.	
10.7.3	Procedures for the physical handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.	All retained documents should be filed and stored in secured file cabinets. Twitter's DocCage policy requires that all retained documents should be filed and stored in secured file cabinets, and, after an appropriate amount of time, all documents should be disposed in official shred bins located throughout the Twitter facilities.	Technical
10.7.4	System documentation should be protected against unauthorized access.	All system documentation is stored on the Twitter wiki. Wiki access requires LDAP authentication, which is only granted to authorized employees and contractors.	Technical
10.8 Exchange of information Objective: To maintain the security of information and software exchanged within an organization and with any external entity.			
10.8.1	Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.	Exchange policies in the Employee Security Handbook strongly recommend securing communication channel with SSL when exchanging password and sensitive information.	Technical
10.8.2	Agreements should be established for the exchange of information and software between the organization	10.8.2.1 Twitter performs a security review of all third party agreements that includes review and	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
	and external parties.	approval by legal and the security team. 10.8.2.2 Additionally, Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security requirements.	
10.8.3	Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.	10.8.3.1 Removable media should not be used to store nonpublic consumer information, unless approved by the Security Team in a ticket. Twitter policy is documented in the Employee Security Handbook, which is communicated, reviewed and confirmed by employees during on-boarding 10.8.3.2 Portable laptops are encrypted with FileVault so as to protect any information if lost.	Technical
10.8.4	Information involved in electronic messaging should be appropriately protected.	Company policy requires users to retain their messages within Google Apps, the electronic messaging for Twitter. Google Apps requires the use of SSL.	Technical
10.8.5	Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.	6.2.3.1 Twitter performs a security review of all third party agreements that includes review and approval by legal and the security team.	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		6.2.3.2 Additionally, Twitter obtains and reviews the vendor's SAS70 or an equivalent report (from an external auditor or the Twitter Security Team) on an annual basis to monitor third party compliance with security requirements.	
10.10 Monitoring Objective: To detect unauthorized information processing activities.			
10.10.1	Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.	User activities, exceptions, and information security events are produced and retained according to an internal data retention policy.	Technical
10.10.2	Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.	Production system logs are processed automatically and the information presented to operations personnel through event-monitoring dashboards.	Technical
10.10.3	Logging facilities and log information should be protected against tampering and unauthorized access.	Only authorized users have access to log systems. Modify access to the log systems is further restricted to a smaller set of authorized users. A quarterly review is conducted of authorized users.	Technical
10.10.4	System administrator and system operator activities should be logged.	Modifications to user data performed using the admin system are logged. Admin logs specify operator and timestamp of activities. The Trust & Safety group monitors and	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		responds to abuse issues.	
10.10.6	The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.	Twitter runs NTP on all machines, which keeps clocks synchronized.	Technical
11.1 Business requirement for access control Objective: To control access to information.			
11.1.1	An access control policy should be established, documented, and reviewed based on business and security requirements for access.	Twitter has implemented policies which govern access provisioning, termination and changes to user access.	Technical
11.2 User access management Objective: To ensure authorized user access and to prevent unauthorized access to information systems.			
11.2.1	There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	11.2.1.1 User access, termination, and modification are granted based on job responsibility as are documented in a ticket. 11.2.1.2 API developer users accept the Twitter API Terms of Service prior to accessing the Twitter systems through the developer API.	Technical
11.2.2	The allocation and use of privileges should be restricted and controlled.	Privileged access to any information system is authorized by the appropriate system manager.	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
11.2.3	The allocation of passwords should be controlled through a formal management process.	Password policy is enforced through training, a formal password policy and system configurations. New passwords are unguessable and allocated to users in a secure fashion. Users must change password on initial login.	Technical
11.2.4	Management should review users' access rights at regular intervals . using a formal process.	LDAP group owners conduct quarterly reviews of user membership to ensure user access is limited. A review of any non-LDAP-based system access controls is conducted on a quarterly basis.	Technical
11.3 User responsibilities Objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.			
11.3.1	Users should be required to follow good security practices in the selection and use of passwords.	High complexity passwords are required for all relevant systems. For LDAP systems, password complexity is enforced. By policy, employees use 1Password or equivalent technology to generate and protect passwords for web services. Additionally, admin passwords are required to be changed semi-annually	Technical
11.3.2	Users should ensure that unattended	Twitter automatically configures a	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
	equipment has appropriate protection.	screensaver policy of 10 minutes or less and additionally there is ad hoc monitoring through Casper of configuration settings.	
11.3.3	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.	Twitter has a clear desk policy that is documented in the Employee Security Handbook.	Technical
11.4 Network access control Objective: To prevent unauthorized access to networked services.			
11.4.1	Users should only be provided with access to the services that they have been specifically authorized to use.	11.4.1.1 User access, termination, and modification are granted based on job responsibility and are documented in a ticket. 11.4.1.2 API developer users accept the Twitter API Terms of Service prior to accessing the Twitter systems through the developer API. 11.4.1.3 Privileged access to any information system is authorized by the appropriate system manager.	Technical
11.4.2	Appropriate authentication methods should be used to control access by remote users.	11.4.2.1 Twitter uses VPN to authenticate remote users. Users have to be part of the VPN group to gain access through VPN.	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		11.4.2.2 User access, termination, and modification are granted based on job responsibility and are documented in a ticket. 11.4.2.3 API developer users accept the Twitter API Terms of Service prior to accessing the Twitter systems through the developer API.	
11.4.3	Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.	Users must authenticate to the corporate network on the local office wifi / LAN or use VPN to access Twitter administrator systems.	Technical
11.4.4	Physical and logical access to diagnostic and configuration ports should be controlled.	11.4.4.1 An electronic access badge is required to enter corporate offices and data centers. Existing controls regarding on-boarding and off-boarding also include procedures for granting and terminating badge access. 11.4.4.2 A quarterly review is conducted of which personnel have access to the data center.	Physical & Technical
11.4.5	Groups of information services, users, and information systems should be segregated on networks.	11.4.5.1 Twitter has implemented policies which govern access provisioning, termination and changes to user access. 11.4.5.2 Twitter utilizes staging servers to separate	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		development and staging environments from the production environment. 11.4.5.3 The corporate network is separated from the data center networks to secure critical production information.	
11.4.6	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications (see 11.1).	11.4.6.1 Twitter has implemented policies which govern access provisioning, termination, and changes to user access. 11.4.6.2 Twitter utilizes staging servers to separate development and staging environments from the production environment. 11.4.6.3 The corporate network is separated from the data center networks to secure critical production information.	Technical
11.4.7	Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.	11.4.7.1 Twitter has implemented network security encryption, firewalls, and VPN protocols to protect the network from threats and inappropriate access. 11.4.7.2 The Network Operations Team configures and monitors the network security in the data centers. The IT Team configures and	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		monitors the network security in the corporate office network. The teams review the security configurations on at least a quarterly basis. 11.4.7.3 The corporate network is separated from the data center networks to secure critical production information.	
11.5 Operating system access control Objective: To prevent unauthorized access to operating systems.			
11.5.1	Access to operating systems should be controlled by a secure log-on procedure.	Twitter has implemented policies which govern access provisioning, termination, and changes to user access.	Technical
11.5.2	All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.	Each user is assigned a unique ID when accessing and performing administration activities on information systems.	Technical
11.5.3	Systems for managing passwords should be interactive and should ensure quality passwords.	High complexity passwords are required for all relevant systems. For LDAP systems, password complexity is enforced. By policy, employees use 1Password or equivalent technology to generate and protect passwords for web services. Additionally, admin passwords are required to be changed semi-annually	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
11.5.4	The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.	All utilities that can override system and application security controls are reviewed before initial deployment to ensure that they conform to security standards. The Ops Manager is responsible to engage the Security Manager to conduct such reviews by submitting a ticket to request a security review.	Technical
11.5.5	Inactive sessions should shut down after a defined period of inactivity.	VPN sessions are configured to timeout after 20 minutes of inactivity.	Technical
11.5.6	Restrictions on connection times should be used to provide additional security for high-risk applications.	VPN sessions have a maximum session length.	Technical
11.6 Application and information access control Objective: To prevent unauthorized access to information held in application systems.			
11.6.1	Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.	11.6.1.1 Twitter has implemented policies that govern access provisioning, termination, and changes to user access. 11.6.1.2 User access, termination, and modification are granted based on job responsibility and are documented in a ticket. 11.6.1.3 API developer users accept the Twitter API Terms of Service prior to accessing the Twitter systems through the developer API.	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
11.6.2	Sensitive systems should have a dedicated (isolated) computing environment.	The corporate network is separated from the data center networks to secure critical production information.	Technical
11.7 Mobile computing and teleworking Objective: To ensure information security when using mobile computing and teleworking facilities.			
11.7.1	A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.	Twitter has a policy to govern mobile computing and teleworking.	Technical
11.7.2	A policy, operational plans, and procedures should be developed and implemented for teleworking activities.	Twitter has a policy to govern mobile computing and teleworking.	Technical
12.1 Security requirements of information systems Objective: To ensure that security is an integral part of information systems.			
12.1.1	Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.	Project design documentation (e.g., the Technical Design Review) for SDLC projects includes, as appropriate, security requirements and input from the Security Team.	Technical
12.2 Correct processing in applications Objective: To prevent errors, loss, unauthorized modification or misuse of information in applications.			
12.2.1	Data input to applications should be	Finance conducts a validation of the accuracy	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
	validated to ensure that this data is correct and appropriate.	of employee data as a part of payroll procedures during on-boarding. HR sends an annual reminder to all employees that they should verify the accuracy of their personal information in the payroll system. When logging in to ADP for the first time, employees must verify their Social Security Number.	
12.2.2	Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	Twitter obtains and reviews the ADP SAS70 on an annual basis to monitor third party compliance with information processing controls.	Technical
12.2.3	Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.	12.2.3.1 Exchange policies in the Employee Security Handbook strongly recommend securing communication channel with SSL when exchanging password and sensitive information. 12.2.3.2 Where message integrity and authenticity is selected for communications between a user and Twitter, SSL is used. When a password is passed between a user and Twitter, SSL is used.	Technical
12.2.4	Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.	Twitter obtains and reviews the ADP SAS70 on an annual basis to monitor third party compliance with information processing controls.	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
12.3 Cryptographic controls Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.			
12.3.1	A policy on the use of cryptographic controls for protection of information should be developed and implemented.	Twitter has a documented policy related to use of cryptographic controls. These include: internal services need to run on SSL (e.g., change management system), SSH protocol used for connections, and API use of cryptography over SSL.	Technical
12.3.2	Key management should be in place to support the organization's use of cryptographic techniques.	SSL certificates are used on applicable products and are issued by a third party. SSL keys for server use are generated using a private key that is stored in an encrypted database restricted to Ops personnel.	Technical
12.4 Security of system files Objective: To ensure the security of system files.			
12.4.1	There should be procedures in place to control the installation of software on operational systems.	All production system changes are documented in the ReviewBoard system, capturing evidence of change approval.	Technical
12.4.2	Test data should be selected carefully, and protected and controlled.	The staging environment utilizes real time production data and is controlled through the same controls as the production environment. Refer to section 11 controls regarding access controls related to systems and data, which includes test data.	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
12.4.3	Access to program source code should be restricted.	All production code is checked into a source code repository system which maintains version history and change logs for all code files. Check in privileges are restricted to authorized users.	Technical
12.5 Security in development and support processes Objective: To maintain the security of application system software and information.			
12.5.1	The implementation of changes should be controlled by the use of formal change control procedures.	All software source code changes are documented in a Review Board ticket, capturing evidence of testing and approval. For all projects, the project team either documents that security has been considered or engages the Security Team, as documented in the Technical Design Review. Conformance to the design review is reviewed and checked in the Production Readiness Review.	Technical
12.5.2	When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Changes to operating systems are tested to validate that there is no adverse impact to the in-scope applications and documented in a Jira ticket.	Technical
12.5.3	Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.	Changes to third-party software packages are applied only when necessary. Any such code changes go through the SDLC process.	Technical
12.5.4	Opportunities for information leakage should be prevented.	12.5.4.1 Twitter has a confidentiality and non-	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		disclosure policy that is required to be read and signed by new hires during their on boarding process. The policy is/are reviewed by HR and Legal on an annual basis. 12.5.4.2 Twitter has implemented policies which govern access provisioning, termination and changes to user access. 12.5.4.2 Twitter has an acceptable use policy and agreement that is signed upon employment and/or issuance of new laptop.	
12.5.5	Outsourced software development should be supervised and monitored by the organization.	If third party software developers are utilized, Twitter monitors and supervise the development work so that it adheres to the security standards of Twitter software.	Technical
12.6 Technical Vulnerability Management Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.			
12.6.1	Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.	12.6.1.1 The IT Group uses to Casper to monitor and update individual operating systems on laptops and ensure that they are a recent version, limiting code vulnerabilities. 12.6.1.2 The Ops Team uses a server management platform (Puppet) to monitor and update	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		operating systems on servers and ensure that they are a secure version. There is a procedure in a testing environment to test patches before deployment.	
13.1 Reporting information security events and weaknesses Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.			
13.1.1	Information security events should be reported through appropriate management channels as quickly as possible.	13.1.1.1 Twitter's Information Security Program policies are centralized in the Employee Security Handbook (including the process for reporting security events). The Security Manager and the Security Committee approves the contents of the Handbook. Policies are communicated via the Wiki site and new hire training. New hires initial sign-in log to confirm attendance of training and review of the Employee Security Handbook. 13.1.1.2 Twitter has a security incident reporting process for external users and employees. External and internal users report issues via security@twitter.com. Directions on how to report are in the employee handbook and on the Twitter website. Incidents are monitored and managed by the Twitter Security and Trust & Safety teams.	Technical
13.1.2	All employees, contractors and third	13.1.2.1	Administrative

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
	party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.	Twitter's Information Security Program policies are centralized in the Employee Security Handbook (including the process for reporting security events). The Security Manager and the Security Committee approves the contents of the Handbook. Policies are communicated via the Wiki site and new hire training. New hires initial sign-in log to confirm attendance of training and review of the Employee Security Handbook. 13.1.2.2 Twitter has a security incident reporting process for external users and employees. External and internal users report issues via security@twitter.com. Directions on how to report are in the employee handbook and on the Twitter website. Incidents are monitored and managed by the Twitter Security and Trust & Safety teams.	
13.2 Management of information security incidents and improvements Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.			
13.2.1	Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.	Twitter has a formal incident management process and policy which is posted on the Wiki. Responsibilities and actions to be taken are detailed in the policy.	Technical
13.2.2	There should be mechanisms in place	A weekly meeting is held to discuss and	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
	to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	monitor incidents.	
13.2.3	Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	Documented evidence is retained by Legal for any incidents involving legal action.	Technical
14.1 Information security aspects of business continuity management Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.			
14.1.1	A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.	The Security Committee considers business continuity procedures as part of its risk assessment considering all possible security events.	Technical
14.1.2	Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security.	The Security Committee considers business continuity procedures as part of its risk assessment considering all possible security events.	Technical
14.1.3	Plans should be developed and implemented to maintain or restore operations and ensure availability of	The Security Committee considers business continuity procedures as part of its risk assessment considering all possible security	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
	information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	events.	
14.1.4	A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.	The Security Committee considers business continuity procedures as part of its risk assessment considering all possible security events.	Technical
14.1.5	Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective.	The Security Committee considers business continuity procedures as part of its risk assessment considering all possible security events.	Technical
15.1 Compliance with legal requirements Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.			
15.1.1	All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.	15.1.1.1 A Legal Team member is assigned to each new product/project. 15.1.1.2 The legal team member performs a legal review of the statutory, regulatory, and contractual requirements for the product/project. Data protection and privacy considerations are part of the legal review. Compliance with relevant cryptographic laws and regulations and agreements is part of the	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		legal review conducted by the Legal Team member of the relevant product/project. Performance of legal review is captured in team meeting notes or in JIRA ticket. 15.1.1.3 An overall legal review, including data protection and privacy considerations, is conducted as part of the annual review by the Security Committee's Legal representative.	
15.1.3	Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.	Important physical records are stored in locked file cabinets, restricted to appropriate personnel on the Legal Team. Important electronic records are stored in a shared directory which is access controlled to Legal Team members.	Technical
15.1.4	Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.	15.1.4.1 A Legal Team member is assigned to each new product/project. 15.1.4.2 The legal team member performs a legal review of the statutory, regulatory, and contractual requirements for the product/project. Data protection and privacy considerations are part of the legal review. Compliance with relevant cryptographic laws and regulations and agreements is part of the legal review conducted by the Legal Team member of the relevant product/project. Performance of legal review is captured in	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		team meeting notes or in JIRA ticket. 15.1.4.3 An overall legal review, including data protection and privacy considerations, is conducted as part of the annual review by the Security Committee's Legal representative.	
15.1.5	Users should be deterred from using information processing facilities for unauthorized purposes.	15.1.5.1 Users use of Twitter is governed by Terms of Service which are reviewed annually by Legal Team. 15.1.5.2 Users' use of Twitter is monitored by Trust & Safety Team for violations of policy using automated abuse detection tools and in response to external complaint process.	Technical
15.1.6	Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations.	15.1.6.1 A Legal Team member is assigned to each new product/project. 15.1.6.2 The legal team member performs a legal review of the statutory, regulatory, and contractual requirements for the product/project. Data protection and privacy considerations are part of the legal review. Compliance with relevant cryptographic laws and regulations and agreements is part of the legal review conducted by the Legal Team member of the relevant product/project.	Technical

ISO Reference	ISO Control Activity Description	Twitter Control Activities	Type of Safeguard
		Performance of legal review is captured in team meeting notes or in JIRA ticket. 15.1.6.3 An overall legal review, including data protection and privacy considerations, is conducted as part of the annual review by the Security Committee's Legal representative.	
15.2 Compliance with security policies and standards, and technical compliance Objective: To ensure compliance of systems with organizational security policies and standards.			
15.2.1	Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.	Managers are responsible for authorizing and maintaining the LDAP groups within their area of responsibility. Any security issues involving an employee are reported to their Manager.	Technical
15.2.2	Information systems should be regularly checked for compliance with security implementation standards.	15.2.2.1 The Security Committee performs an annual review of the overall Information Security Program. As an input to that review, the security team will select controls for testing based on a plan and will validate that the remaining untested controls are in place.	Technical

II. Third-Party Developer Access to the Twitter API

An Application Programming Interface ("API") is a defined way for a program to accomplish a task, usually by retrieving or modifying data. Twitter provides an API method for just about every feature visible on the Twitter website, including the DM feature. Third-party programmers can use the Twitter API to make applications and websites that interact with Twitter. Their programs talk to the Twitter API over HTTP, the same protocol used by browsers to visit and interact with web pages. The Twitter API includes a REST API, a Streaming API, and a Search API. For the Search API, no authentication is required since the information provided by the Search API is publicly available. For the REST API and the Streaming API, an Application Permission Model is used to control access to DMs.

In order for a developer to create an application that can access information such as a user's DMs, the developer must:

- agree to the Twitter Terms of Service (https://twitter.com/tos);
- agree to the Developer Rules of the Road (https://dev.twitter.com/terms/api-terms);
- obtain a consumer key; and
- obtain a consumer secret.

The developer must specifically agree to the Twitter Terms of Service in order to obtain an account. Once logged into their account, the developer must specifically agree to the Developer Rules of the Road in order to obtain a consumer key and a consumer secret generated by Twitter. Notably, it is a principle in the Developer Rules of the Road to "[r]espect user privacy" and that Twitter may immediately suspend a developer's credentials including their consumer key and consumer secret for any violations of the Rules.

API developer users accept the Twitter API Terms of Service prior to accessing the Twitter systems through the developer API. (Twitter Control 11.2.1.2)

Twitter utilizes the OAuth protocol to control access to user data by third-party developers. The API documentation details Twitter's security implementation requirements. Any API changes that could affect security of information protected by the API are reviewed for approval by the Security Team, and by the Legal Team if they also impact existing policies, agreements, or terms. (Twitter Control 10.2.1.2) Twitter monitors operational activities to identify large scale API inappropriate activity. Inappropriate activity will result in API shutdown. (Twitter Control 10.2.2.1)

III. The Company did not include Tweetdeck, AdGrok, Back Type, or BagCheck in the scope of the assertion.