Chris Hoofnagle  
UC Berkeley School of Law  
344 Boalt Hall,  
Berkley, CA 94720

Re: FOIA-2016-00063  
TrendNet

Dear Mr. Hoofnagle:

This is in response to your request dated October 09, 2015, under the Freedom of Information Act seeking access to communications between the FTC and Trendnet Corporation or its counsel between September 24, 2014 and September 24, 2015. In accordance with the FOIA and agency policy, we have searched our records as of October 09, 2015, the date we received your request in our FOIA office.

We have located 62 pages of responsive records. I am granting partial access to the accessible records. 2 pages and portions of other pages fall within 2 of the exemptions to the FOIA’s disclosure requirements, as explained below.

Some pages and portions of other pages constitute confidential commercial or financial information, which is exempt from disclosure under FOIA Exemption 4, 5 U.S.C. § 552(b)(4). See Critical Mass Energy Project v. NRC, 975 F.2d 871, 879 (D.C. Cir. 1992). Moreover, because Section 6(f) of the FTC Act, 15 U.S.C. § 46(f), prohibits public disclosure of this type of information, it is also exempt under FOIA Exemption 3, 5 U.S.C. § 552(b)(3), which exempts from disclosure any information that is protected from disclosure under another federal statute.

If you are not satisfied with this response to your request, you may appeal by writing to Freedom of Information Act Appeal, Office of the General Counsel, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington D.C. 20580, within 30 days of the date of this letter. Please enclose a copy of your original request and a copy of this response. If you believe that we should choose to disclose additional materials beyond what the FOIA requires, please explain why this would be in the public interest.
If you have any questions about the way we handled your request or about the FOIA regulations or procedures, please contact Katie Baker at 202-326-2869.

Dione J. Stearns
Assistant General Counsel

Enclosed: CD
Please add the e-mails below to the Order Enforcement database for the matter **Trendnet, Inc., Matter # C4426.**

Thanks,

Artie

---

**From:** Brian Chu  
**Sent:** Friday, January 16, 2015 5:45 PM  
**To:** Decastro, Arturo  
**Cc:** Pei Huang; Peggy Huang; Sonny Su; johnlsun@att.net  
**Subject:** FW: Trendnet Initial Assessment Report

Dear Artie,

Please expect the report at the specified time. Thank you for your clarifications.

Brian Chu  
IT Director

[TRENDnet](http://www.trendnet.com)  
20675 Manhattan Place, Torrance, CA 90501, USA  
Tel: 310-961-5477 Fax: 310-961-5511  
Email: b.chu@trendnet.com  
Web: [www.trendnet.com](http://www.trendnet.com)  
Where to Buy: [www.trendnet.com/sales](http://www.trendnet.com/sales)

---

**From:** Decastro, Arturo  
**Sent:** Friday, January 16, 2015 2:19 PM  
**To:** 'b.chu@trendnet.com'; 's.su@trendnet.com'  
**Cc:** 'John L. Sun'  
**Subject:** Trendnet Initial Assessment Report

Dears Messrs. Chu and Su:

Thank you again for speaking with me this afternoon. This is to confirm that Trendnet can submit to the FTC a Supplemental Initial Assessment Report ("Supplemental Report"), which better addresses Sections III.A-D of the Consent Order along the lines we discussed, by **January 30, 2015**
(two weeks from today). The Supplement Report should be submitted by overnight courier or e-mail as prescribed by Section III of Order.

If you have any questions, please don’t hesitate to contact me.

Best regards,

Artie DeCastro

Arturo DeCastro
Federal Trade Commission
BCP-Division of Enforcement
600 Pennsylvania Avenue, NW
Mail Drop CC-9528
Washington, DC 20580
202-326-2747
202-326-3197 (Fax)
DEbrief

From: Decastro, Arturo
Sent: Wednesday, January 28, 2015 9:08 AM
To: DEbrief
Subject: FW: Trendnet Initial Assessment Report

Please add these e-mails to the database for the matter **Trendnet, C4426**.

Thanks.

---

From: Brian Chu [mailto:b.chu@trendnet.com]
Sent: Monday, January 26, 2015 5:53 PM
To: Decastro, Arturo
Cc: 'Sonny Su'; johnsun@att.net
Subject: RE: Trendnet Initial Assessment Report

Hi Artie,

We are certain you will receive the supplemental report before 2/6 as soon as it’s completed. Thank you for your understanding.

Brian

---

From: Decastro, Arturo [mailto:adecastro@ftc.gov]
Sent: Monday, January 26, 2015 2:49 PM
To: Brian Chu
Cc: Sonny Su; johnsun@att.net
Subject: Re: Trendnet Initial Assessment Report

Dear Mr. Chu:

Thank you for the update. I would not recommend any action to my supervisors if Trendnet submitted the report on 2/6 instead of 1/30. Thanks again, and we look forward to seeing the supplemental report.

Regards,

Artie

---

On: 26 January 2015 16:36, "Brian Chu" [mailto:b.chu@trendnet.com] wrote:

Dear Artie,

Our security consultant is asking if we could get the deadline extended to 2/6 (Fri). They would like to include additional information on the supplement report.
Please let me know your response as soon as possible.

Thank you for your understanding.

Brian

From: Brian Chu [mailto:b.chu@trendnet.com]
Sent: Friday, January 16, 2015 2:45 PM
To: 'adecastro@ftc.gov'
Cc: Pei Huang; Peggy Huang; Sonny Su; 'johnsun@att.net'
Subject: FW: Trendnet Initial Assessment Report

Dear Artie,

Please expect the report at the specified time. Thank you for your clarifications.

Brian Chu
IT Director
20675 Manhattan Place, Torrance, CA 90501, USA
Tel: 310-961-5477 Fax: 310-961-5511
Email: b.chu@trendnet.com
Web: www.trendnet.com
Where to Buy: www.trendnet.com/sales

From: DeCastro, Arturo [mailto:adecastro@ftc.gov]
Sent: Friday, January 16, 2015 2:19 PM
To: 'b.chu@trendnet.com'; 's.su@trendnet.com'
Cc: 'John L. Sun'
Subject: Trendnet Initial Assessment Report

Dear Messrs. Chu and Su:

Thank you again for speaking with me this afternoon. This is to confirm that Trendnet can submit to the FTC a Supplemental Initial Assessment Report (“Supplemental Report”), which better addresses Sections III.A-D of the Consent Order along the lines we discussed, by January 30, 2015 (two weeks from today). The Supplement Report should be submitted by overnight courier or e-mail as prescribed by Section III of Order.

If you have any questions, please don’t hesitate to contact me.

Best regards,

Artie DeCastro

Arturo DeCastro
Statement for Introducing Security Program within TRENDnet

Jia-Chyi Wu, jiachyi@iii.org.tw

Security Evaluation and Assurance Lab (SEAL), Director

Kuang-Chun Hung, morgan.hung@iii.org.tw

Security Evaluation and Assurance Lab (SEAL), Manager

Institute for Information Industry

Dear Sirs/Madam,

Security Evaluation and Assurance Lab functions as an independent security testing laboratory within Institute for Information Industry, also providing qualified security services to help the Internet and network communication vendors in dealing with security challenges.

Be one of security specialist within SEAL, Jia-Chyi Wu with Certified CISSP, BSI 7799 Lead Auditor and ISO 20000 Lead Auditor certificates, and Kuang-Chun Hung with Certified GIAC GPEN, GIAC GREM, EC Council CEH and EC Council CHFI certificates, in charge of security enabling project and prepared a set of security-related policies, guidance, and procedures for TRENDnet, aiming to assist TRENDnet in mitigating security risks target on organization and promoting products quality and security level. As for the security framework introduced to TRENDnet, security artifacts listed in the Appendix A have already been defined and a number of security aspects were developed based on an international standard called ISO/IEC 27001.
Overall, computer usage, document classifying, and related security policies for the TREDNnet organization itself have been deployed, tasks for classifying documents, doing risk assessment, providing security awareness training to employees, and perform internal audits were on progress. In addition, to defend against attacks target on network products and to protect consumers' credentials and data, several additional security controls and operation document for outsourced product and outsourced service were defined. On top of that, all outsourced products will be requested to do security assessment, corresponded reports will be reviewed as well during acceptance check process to ensure there is no high-level above severity vulnerabilities exist.
## Contents

1. Executive Summary ................................................................. 1

2. Background and Introduction .................................................. 3
   2.1. FTC Order Requirements .................................................. 3
   2.2. Requirement and Qualification of III Auditors ....................... 5
   2.3. Procedures and standards used for assessment and audit .......... 8

3. Objective and Normative References ......................................... 11
   3.1. Audit Objective of TRENDDnet ......................................... 11
   3.2. Normative References of TRENDDnet ............................... 15
   3.3. Audit Scope .................................................................... 15
   3.4. Timing ........................................................................... 18

4. Good Practices and Records of Security Program ......................... 21

5. Summary of First Audit Findings ............................................... 38

6. Summary of Second Audit ......................................................... 40

7. Conclusion ............................................................................. 41

8. References ............................................................................. 43

9. Appendix ................................................................................. 44
9.1 Appendix A Detail of First Audit Findings

44
List of Figures

Figure 1  III Project Organization and Tasks .................................................. 7
Figure 2  TRENDSnet Audit Scope .................................................................. 17
I. Executive Summary

The Institute for Information Industry (hereinafter “III”) has prepared this report pursuant to Part III of the Federal Trade Commission’s (“FTC’s”) Decision and Order - In the Matter of TRENDnet, Inc. (hereinafter the “TRENDnet”) (FILE NO. 122 3090) (hereinafter the “FTC Order”). III conducted the audit to review TRENDnet’s implementation of a comprehensive security program for safeguarding TRENDnet’s Covered Device, Covered Device Functionality, and Covered Information Systems (terms as defined in the FTC Order) in compliance with Part II of the FTC Order. For completeness of assessment, III conducted two audits covering the reporting period of July 1th, 2014 to January 28th, 2015.

III conducted its first audit from January 19th to January 21th, 2015. III performed an overall examination of the effectiveness and sufficiency of security safeguards that TRENDnet implemented, and identified areas for improvement. The second audit was scheduled from January 26th to January 28th, 2015 to ensure the completeness and integrity of the first audit, and to assess the effectiveness of TRENDnet’s improvement plan with regard to the findings identified in the first audit.
III summarized the results of the first audit and proposed that TRENDnet ensure a continuous improvement plan for certain security areas for continued compliance with the FTC Order. TRENDnet then enhanced security controls aiming for the improvement of security safeguards. III then conducted the second audit confirming that TRENDnet had appropriately enhanced the security controls.

In conclusion, III hereby certifies that TRENDnet has implemented a security program with sufficient effectiveness to provide reasonable assurance that the security of Covered Devices, Covered Device Functionality and Covered Information is protected and has so operated throughout the reporting period, in compliance with Part II of the FTC Order.
2. Background and Introduction

2.1. FTC Order Requirements

This report is pursuant to the Federal Trade Commission’s Decision and Order - *In the Matter of TRENDnet Inc.* (FILE NO. 122 3090).

According to the Part II of the FTC Order, TRENDnet (the “respondent”) should establish and implement a comprehensive security program that is reasonably designed to (1) address security risks that could result in unauthorized access to or use of Covered Device Functionality, and (2) protect the security, confidentiality, and integrity of Covered Information, whether collected by TRENDnet or input into, stored on, captured with, accessed, or transmitted through a Covered Device. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to TRENDnet’s size and complexity, the nature and scope of TRENDnet’s activities, and the sensitivity of the Covered Device Functionality or Covered Information, as described in sections A to H.

Furthermore, Part III of the FTC Order requests that TRENDnet, in connection with its compliance with Part II of this Order, shall 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. Professionals qualified to prepare such
Assessments shall be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience programming secure Covered Devices or other similar Internet-accessible consumer-grade devices; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and in programming secure Covered Devices or other similar Internet-accessible consumer-grade devices; or a similarly qualified person or organization; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred eighty (180) days after service of the order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

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

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 Covered Device Functionality or Covered Information;

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

D. Certify that respondent’s security program is operating with sufficient
effectiveness to provide reasonable assurance that the security of Covered Device Functionality and the security, confidentiality, and integrity of Covered Information is protected and has so operated throughout the reporting period.

2.2. Requirement and Qualification of III Auditors

III was founded in 1979. III's goal is to facilitate and motivate the development of Taiwan's Information and communications technology (ICT) industry and to promote the deployment of ICT in public and private sectors. III has 33 years of steady growth and proactive contribution to the development of Taiwan's ICT industry and information society, especially in the fields of software development, information security, and development.

In January 2015, III proposed a professional team with members that are competent and experienced to work on this project. Most members have over ten years working experience in IT information security fields, with certifications including Certified Secure Software Lifecycle Professional (“CSSLP”), Certification Information System Security Professional (“CISSP”), ISO 27001 Lead auditor, and other relevant certifications.

For details of the qualifications, refer to Table 1 below:
Table 1 – List of Audit Team Members

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Key Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jia-Chyi Wu</td>
<td>Project manager</td>
<td>Coordination and management of the project and responsible for ensuring that the audit team complete the project. (CISSP, BS 7799 LA and ISO 20000 LA certified)</td>
</tr>
<tr>
<td>Wei-Chieh Yang</td>
<td>Audit Team member</td>
<td>Security audit. (GCIA, GSSP-JAVA, SSCP, SCJP, ISO 20000 LA certificated)</td>
</tr>
<tr>
<td>Zong-Lin Tsai</td>
<td>Audit Team member</td>
<td>Security audit. (CISSP, CSSLP, CEH, OCP, OCA, RHCE, SCWCD, SCJP certified)</td>
</tr>
</tbody>
</table>

Data Source: III

The III project team has a two-tier structure: (1) The leader is Jia-Chyi Wu, with more than 15 years of experience in ICT project management fields, and (2) The three functional teams: the assessment team, the audit team and the legal team respectively, with the project manager Wei-Chieh Yang who is specialized in IT-related fields, i.e. Security Development Lifecycle (SDL) and auditing. The organization chart and personnel assignment is shown in Figure 1.

• Audit team
  – analyze the TRENDnet's IT framework
- prepare the working materials with ISO 27001:2013
- assess the security program with reference to the requirements of the FTC Order
- review of the corrective action and preventive action after audit
- propose audit opinions and recommendations for the security program
- process review of vulnerability assessment and testing
- review of security related records
- review the Final report

![Project Organization and Tasks](image)

Figure 1  III Project Organization and Tasks

Data Source : III
2.3. Procedures and standards used for assessment and audit

Using the industry-accepted security and security management framework that TRENDnet has adopted for the basis of its security program, ISO 27001:2013, III has designed an assessment and audit worksheet to comprehensively review and assess TRENDnet’s security program, as required by Part II of the FTC Order.

The following paragraph lists the focal points and topics of the audit related to and ISO 27001:2013.

**ISO 27001: 2013**

TRENDnet uses the ISO 27001:2013 framework for the security program. ISO 27001:2013 is an information security management system framework published by ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission). The requirements set out in ISO 27001:2013 provide a model for establishing, implementing, operating, monitoring, reviewing and improving an Information Security Management System. Following the requirements of this international standard, III assessed the security controls that TRENDnet has implemented to manage the information security risk, and protect security, confidentiality, and integrity of Covered Information. III has also applied the ISO 27001 PDCA Model (Plan, Do, Check, Act) to examine the compliance and effectiveness of information security system [1]. The following management domains were selected from
ISO 27001:2013 to review the control objectives and controls of TRENDnet security safeguards.

- Security policy, to review information security policy.

- Organization of information security, to review information security within the audit scope.

- Asset management, to ensure that information receives an appropriate level of protection.

- Human resources safeguards, implemented in the form of security training for all relevant personnel to identify, understand and be aware of information security threats, risks and concerns and understand their responsibilities respecting safeguarding Covered Information and Covered Device.

- Physical and environmental security, to check the authorized physical access, damage and interference about premises and information.

- Communication and operations management, to ensure the correct and secure operation of information processing facilities, integrity of software and information.

- Access control, to check the access control of Covered Information and Covered Device Functionality, preventing compromise of network services, application systems information and information processing facilities.
- Information development and maintenance, to ensure that security is an integral part of information systems.

- Information security incident management, to ensure that security events and threats associated with Covered Information and Covered Devices are communicated and corrective action is taken in a timely manner.

- Compliance, to review any possible breaches of law, regulatory or contractual obligations, and of any security requirements.
3. Objective and Normative References

3.1. Audit Objective of TRENDnet

III developed audit objectives based on the requirements of the FTC Order as listed as below:

- Assess and document how the safeguards that have been implemented meet or exceed the protections required by Part II of the FTC Order as follows:

A. The designation of an employee or employees to coordinate and be accountable for the security program;

B. The identification of material internal and external risks to the security of Covered Devices that could result in unauthorized access to or use of Covered Device Functionality, and assessment of the sufficiency of any safeguards in place to control these risks;

C. The identification of material internal and external risks to the security, confidentiality, and integrity of Covered Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in respondent’s possession or is input into, stored on, captured with, accessed, or transmitted through a Covered Device, and assessment of the sufficiency of any safeguards in place to control these risks;

D. At a minimum, the risk assessments required by Subparts B and C should
include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) product design, development, and research; (3) secure software design, development, and testing; and (4) review, assessment, and response to third-party security vulnerability reports;

E. The design and implementation of reasonable safeguards to control the risks identified through the risk assessments, including but not limited to reasonable and appropriate software security testing techniques, such as: (1) vulnerability and penetration testing; (2) security architecture reviews; (3) code reviews; and (4) other reasonable and appropriate assessments, audits, reviews, or other tests to identify potential security failures and verify that access to Covered Information is restricted consistent with a user’s security settings;

F. Regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures;

G. The development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order, and requiring service providers, by contract, to establish and implement, and thereafter maintain, appropriate safeguards consistent with this order; and

H. The evaluation and adjustment of the security program in light of the results of the testing and monitoring required by Subpart F, any material changes to the respondent’s operations or business arrangements, or any other
circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its security program.

• To review and document the specific administrative, technical, and physical safeguards that TRENDnet has implemented and maintained during the reporting period to:
  
  – Address security risks related to the development and management of new and existing Covered Device.
  
  – Protect the security, confidentiality, and integrity of Covered Information, whether collected by respondent or input into, stored on, captured with, accessed or transmitted through a Covered Device.
  
  – Assess and document how safeguards are appropriate to TRENDnet’s size and complexity, the nature and scope of TRENDnet’s activities, and the sensitivity of the Covered Device Functionality or Covered Information.

To ensure the designed security program meets the requirements of the FTC Order, III has categorized the following three main areas to examine the consistency with the documented procedures and daily operations related to the nature and scope of TRENDnet’s activities.

• Risk identification & assessment
- Roles and responsibilities
- Documented procedures for the security program
- Training programs
- third party vendor management with product and software design
- PII (Personally identifiable information) Inventory
- Vulnerability information gathering

* Design and implementation of risk controls
  - Regular testing or monitoring of the effectiveness of the safeguards' key controls, systems and procedures
  - Evaluation and adjustment of the security program

* Plan-Do-Check-Act process of security program
  - Measurement of real processes' consistency with documented procedures
  - Measurement of effectiveness and efficiency of regulatory processes, control methods, systems and procedures

*To certify if TRENDnet has demonstrated it has implemented a security program that is operating with sufficient effectiveness to provide reasonable assurance that the security of Covered Device Functionality and the security, confidentiality, and integrity of Covered Information is protected and has so
operated throughout the reporting period, in compliance with Part II of the FTC Order.

3.2. Normative References of TRENDnet

- ISO/IEC 27001:2013 Information technology - Security techniques – “Information security management system” requirements. This is the formal specification for an ISMS against which organizations may be certified compliant.[1]

3.3. Audit Scope

III, as an independent third party audit team, examines the comprehensive security program of TRENDnet under the scope of the FTC Order. The period of audit sample selection was from 1\textsuperscript{st} July, 2014 to 28\textsuperscript{th} January, 2015. Occasionally, the sample selection might be earlier than the date of 1\textsuperscript{st} July, 2014, for the purpose of reviewing consistent management processes. The audit included interviews with executives and function teams, conducted mostly con-call, with supplemental communications via e-mail or phone and review of documentation. The audit domain included Covered Device, Covered Information and Covered Device Functionality, to understand and analyze the compliance level of administrative, technical and physical safeguards. III formed an assessment team to analyze the TRENDnet’s IT framework, the main purpose was to ensure the selection of TRENDnet representative function teams meets the scope requirement of Covered Device, Covered Information and Covered
Device Functionality. Within TRENDnet, two major security teams, (to be replacement with Security team), have established the framework of the whole security program with Covered Device, Covered Information and Covered Device Functionality.

TRENDnet has assembled information security team. Mr. Brian Chu and Mr. Sonny Su are designated employees to coordinate and accountable for the security program. All the function teams were audited from 19th January to 28th January, 2015.
The following chart outlines the audit scope of TRENDnet:

![TRENDnet Audit Scope Diagram]

Figure 2  TRENDnet Audit Scope

Data Source : III

3.3.1.1. Audit Scope of Covered Device

The audit scope includes the review of the administrative, technical and physical safeguards across internal function teams of the ISMS Security Team and related sections within the Covered Device function. The following table outlines the preliminary audit scope of Covered Device functions:
Table 2 – Audit scope of Security team

<table>
<thead>
<tr>
<th>Function Team</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sonny Su, Wen Tasi</td>
<td>Thirty party Vendor Management</td>
</tr>
<tr>
<td>Brian Chu, Anne Kissel</td>
<td>Physical Security</td>
</tr>
<tr>
<td>Sonny Su, Brian Chu, Anne Kissel</td>
<td>Security Incident Responses</td>
</tr>
<tr>
<td>Sonny Su, Brian Chu</td>
<td>Documented Procedure</td>
</tr>
<tr>
<td>Brian Chu, Anne Kissel</td>
<td>Training Programs</td>
</tr>
<tr>
<td>Sonny Su, Brian Chu, Anne Kissel</td>
<td>Risk Identification and Assessment</td>
</tr>
<tr>
<td></td>
<td>Regular Testing/Monitoring of the Effectiveness of the Safeguards’ Key Controls, Systems, and Procedures</td>
</tr>
<tr>
<td>Sonny Su, Brian Chu, Anne Kissel</td>
<td>Evaluation of Adjustment of the Security Program</td>
</tr>
</tbody>
</table>

Data Source: III

3.4. Timing

3.4.1. First Audit

III conducted the first audit from 19th January, to 21st January, 2015. Table 3 illustrates the functional teams that III audited and the audit schedule.
Table 3 – TRENDnet First Audit Schedule

<table>
<thead>
<tr>
<th>Function team</th>
<th>Audit Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pei Huang, Sonny Su, Brian Chu</td>
<td>Audit duration • 1/19/2015~1/21/2015</td>
</tr>
<tr>
<td></td>
<td>Audit duration</td>
</tr>
<tr>
<td></td>
<td>ISO/IEC 27001:2013</td>
</tr>
<tr>
<td></td>
<td>&quot;Information security management system&quot;</td>
</tr>
<tr>
<td></td>
<td>requirements</td>
</tr>
<tr>
<td></td>
<td>Information security</td>
</tr>
<tr>
<td></td>
<td>normative references</td>
</tr>
<tr>
<td></td>
<td>TRENDnet Audit executive plan</td>
</tr>
</tbody>
</table>

Data Source : III
### 3.4.2. Second Audit

**Table 4 – TRENDnet Second Audit Schedule**

<table>
<thead>
<tr>
<th>Function team</th>
<th>Audit duration</th>
<th>Audit Detail</th>
</tr>
</thead>
</table>
| Pei Huang, Sonny Su, Brian Chu | 1/26/2015–1/28/2015 | • ISO/IEC 27001:2013 “Information security management system” requirements  
• Information security normative references  
• TRENDnet Audit executive plan  
• TRENDnet Preliminary Report |

Data Source: III
4. Good Practices and Records of Security Program

TRENDnet has implemented an appropriate security program designed to (1) address security risks related to the development and management of new and existing Covered Device, and (2) protect the security, confidentiality, and integrity of Covered Information, whether collected by TRENDnet or input into, stored, captured with, accesses or transmitted through a Covered Device.

III followed the audit interviews with a review of TRENDnet records relating to the TRENDnet security program, including a review of documentation and processes described in relating to Covered Device, Covered Information, and relating to Covered Device Functionality. Through III’s interviews and review of records, III determined that TRENDnet has implemented the practical safeguards with regard to the administrative technical and physical controls appropriate to TRENDnet’s size and complexity, the nature and scope of TRENDnet’s activities, and the sensitivity of the Covered Device Functionality or Covered Information, as described in the good practices in section A to H below.

• FTC Order Part II - A. The designation of an employee or employees to coordinate and be accountable for the security program;
  - TRENDnet has formed the Security team, led by TRENDnet Mr. Brian Chu
and Mr. Sonny Su. The senior director of Information Technology also serves as the executive secretary managing cross-collaboration of all function teams.

- The ISMS Security team leads the FTC Governance Team, responsible for ensuring TRENDnet's compliance with global privacy and security regulatory requirements, communication of security issues to customers and recording security issues in TRENDnet internal tracking system.

- Assigned security groups are in charge of security programs for software security and information security. The security team members have the required competencies and experience to manage TRENDnet's safeguards.

- The ISMS Security team takes the authority and responsibility to build the framework of security governance across functional teams and business partners that take part in the development of Covered Device and Covered Device Functionality.

- The ISMS Security team takes the authority and responsibility to protect the security, confidentiality, and integrity of Covered Information, by developing and publishing enterprise level security control documents including security policies and implementing processes for protection of information systems, facilities and sensitive information data.
• FTC Order Part II - B. The identification of material internal and external risks to the security of Covered Devices that could result in unauthorized access to or use of Covered Device Functionality, and assessment of the sufficiency of any safeguards in place to control these risks;

- TRENDnet has built an Application Security Management Policy used as the basis for the identification and mitigation of security risks.

- TRENDnet has implemented a high level security risk assessment process to identify and mitigate material internal and external risks to the security of Covered Device.

- TRENDnet has developed and published documented guidelines for identification, classification and protection of Covered Information.

- TRENDnet has developed a security risk assessment process in the form of a risk questionnaire to identify and mitigate internal and external risks to the security of Covered Device Functionality.

- TRENDnet’s ISMS security team is charged and responsible for the identification of material internal and external risks to the security of Covered Devices that could result in unauthorized access to or use of Covered Device Functionality.

- TRENDnet has already retained third party experts to assess the sufficiency
of any safeguards in place to control risks.

- TRENDnet has adopted a capable framework of risk identification and assessment program such as risk identification, analysis and response to manage risks.

➢ TRENDnet's risk assessment questionnaire is designed for the identification and classification of risk relating to Covered Device Functionality.

- TRENDnet has requested vendor supplied to TRENDnet to implement reasonable safeguards to control the risks identified through the risk assessment, such as IP cam. The result of vendor's risk assessment will be forward to third-party expert for further review to identify potential security failures and verify that access to Covered Information is restricted consistent to user's security settings

- The risk assessments required by Subparts B and C include consideration of risks in each of relevant operation, including, but not limited to: (1) employee training and management; (2) product design, development, and research; (3) secure software design, development, and testing; and (4) review, assessment, and response to third-party security vulnerability report

- TRENDnet ISMS Security team and product manager have been conducting and will continue to conduct testing of the effectiveness of the
safeguards' key controls, systems and procedures.

- TRENDnet has published on its web based helpdesk system to receive and monitor feedbacks from its customers and uses and conduct further assessment of effectiveness of the safeguards’ key controls, systems, and procedures.

- TRENDnet has discontinued affected products until the security meeting the new security requirement.

- TRENDnet has required vendors that responsible for high risk products to conduct testing in consistent with this Order and to provide test report to TRENDnet.

**FTC Order Part II - C. The identification of material internal and external risks to the security, confidentiality, and integrity of Covered Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in respondent's possession or is input into, stored on, captured with, accessed, or transmitted through a Covered Device, and assessment of the sufficiency of any safeguards in place to control these risks;**

- TRENDnet has implemented a process to conduct the risk assessments
related to the control objectives and controls of ISO 27001:2013 to measure the risk level of Covered Information.

- As part of its risk assessment process, TRENDnet has developed a risk questionnaire to help identify the appropriate security risk level of Covered Information and appropriate controls are followed to mitigate the identified risks.

- TRENDnet has implemented and published an Information Security Policy that requires identification and assessment of Covered Information to ensure appropriate security and protection for all data and information in its control domain of ownership.

- TRENDnet has developed and published documented guidelines for identification, classification and protection of PII (as defined in the FTC
Order). All the guidelines are reviewed and unified by the ISMS Security team to meet the compliance obligations.

*FTC Order Part II- D. At a minimum, the risk assessments required by Subparts B and C should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) product design, development, and research; (3) secure software design, development, and testing; and (4) review,
assessment, and response to third-party security vulnerability reports;

The risk assessments required by subparts B and C included identification of related operations for TRENDnet, its Covered Device, Covered Information and Covered Device Functionality with consideration of risks in each area of relevant operation. The identified operations and associated risks for Covered Devices, Covered Device Functionality and Covered Information were assessed according to the methodology of risk assessment of ISO 27001 standard.

- (D1) TRENDnet has identified the requirements of security training programs to assess the adequacy of its training programs and whether are designed for team members and new staff in accordance with their roles and needs.

- (D2) For the identification of risks related to product design, development, and research. TRENDnet takes the of who recommends security programming guidelines, performs programming codes reviews, conducts white/black hat security testings. All the security controls will be cooperated with TRENDnet ISMS team.

- TRENDnet ISMS collect security reports issued by other sources such as business partners, customers, and Internet news outlets. Reports are forwarded to third-party Security consultant and/or product vendors for further review.
(D4) Under the methodologies of risk assessment, TRENDnet identified the need related to consider risk relating to handling of third party vulnerability reports. The ISMS security team will assess the security report provided by its vendors. TRENDnet security team will review and assess any news or reports that appear on the Internet relating to security vulnerability of similar devices..

• FTC Order Part II - E. The design and implementation of reasonable safeguards to control the risks identified through the risk assessments, including but not limited to reasonable and appropriate software security testing techniques, such as: (1) vulnerability and penetration testing; (2) security architecture reviews; (3) code reviews; and (4) other reasonable and appropriate assessments, audits, reviews, or other tests to identify potential security failures and verify that access to Covered Information is restricted consistent with a user's security settings;

The following summary shows that TRENDnet has achieved an acceptable maturity level of security assurance.

- TRENDnet formed a ISMS Security team to enhance software and information security and eagerly formed a security culture across internal teams.
- TRENDnet has adopted ISO 27001:2013 to develop the basis of its security framework.

- Following the best practice of ISO 27001 standard, TRENDnet has implemented information security policies and procedures as part of a comprehensive security program.

- TRENDnet developed role based training to ensure the understanding of security design and improve the capabilities of secure software development for its personnel.

- TRENDnet implemented processes for the design and implementation of safeguards to manage security risks related to development and management of high risk Covered Devices, such as IP cam products.

- TRENDnet has developed security controls such as the source code review, security testing and penetration testing with outsourcing security consultant to operate effectively to identify security risks and improve the process of software development.

- TRENDnet developed a process to ensure that the firmware of the Devices have to be approved by the Security team. The Security team ensures the Devices firmware implements software risk mitigation best practices and follows Outsourced Product Management.

- TRENDnet has developed a management process to help ensure secure
software design. TRENDnet developed software security baseline to cover the data usage lifecycle, including data input into, stored on, captured with, accessed or transmitted through a Covered Devices.

- TRENDnet’s built a management process for security testing using both unplanned and periodically scheduled testing with outsourcing security consultant.

- TRENDnet identifies and classifies Covered Information through a risk identification and analysis processes.

- TRENDnet has implemented information classification and protection guidelines. TRENDnet classifies data by sensitivity level and assigns its corresponding protections.

- TRENDnet has established a management process for updating patches for those affected platforms and releasing patches on the website for affected customers’ devices. Additionally, any information related to incidents will be taken as lessons learned. These related security control methods will be feedback to the security requirement to ensure secure software design.

- All the relevant progress to respond to security issues, including from third party vulnerability reports, and improve the security program is controlled and tracked. Security incidents related to discovered vulnerabilities are handled in a maintenance release process and escalated to related
management.

- System and facilities managers check the account's validation monthly to ensure the accuracy of access rights. TRENDDnet has built centralized management of documented procedures and sharing of security resources.

This includes the following information:

➤ Guidelines and standard operation procedure

➤ Outsourcing Service Management

➤ System Security Management

➤ Information classification and protection rules

➤ Application Security Management

➤ Outsourced Product Development

- TRENDDnet has implemented and published a product security channel for direct reporting of security incidents and vulnerabilities by third parties. A security incident response program has been built for event and incident response and collection and tracking of information relating to investigation and resolution of incidents gathered from partners, internal staff, customers and so on. The security incident response program provides an effective management process for receiving, allocating and responding to any issues and security incidents related to Covered Device,
Covered Information and Covered Device Functionality.

- TRENDnet has appropriately adopted the framework of ISO 27001:2013 to implement security management processes such as information security policy, risk management process and security SOPs in order to address security risks relating to the security requirements of confidentiality, integrity and protection during Covered Information use, transmission, storage and disposal including through the following management domains:

➤ Security Policy

TRENDnet has published an information security policy and information classification standards and communicated these policies and standards to employees who handle Covered Information.

➤ Organization of Information Security

TRENDnet’s manages information security and its implementation such as controls, policy, processes, and procedures for information security through designated personnel and outside consultants.

➤ Asset Management

TRENDnet has implemented an information classification standard and asset management processes to ensure TRENDnet personnel follow the safeguarding, handling, disposal, and security requirements associated with the TRENDnet classification and protection levels.
Physical and Environmental Security

TRENDnet has implemented security perimeters such as card controlled entry gates to protect areas that contain Covered Information and Covered Information processing facilities from unauthorized access, destruction, loss, or other unauthorized use or activities...

Communications and Operations Management

TRENDnet has implemented the secure network architecture, and the network segments and configurations of network devices set based upon industry best practices.

- TRENDnet ensures protections such as encryption and transport layer protection as security requirements during the design stage of Covered Information system development.

Access Control

TRENDnet has implemented a formal account registration and de-registration procedures for granting and revoking access to information systems and services. And the related records and control are well implemented with the physical and technical protection.

Information System Development and Maintenance

TRENDnet implements effective security practices relating to protection...
of Covered Information including in the following areas:

- To ensure the protection of Covered Information, security assessment and testing are conducted for Covered Information systems periodically.

➢ Information Security Incident Management

TRENDnet has implemented a security incident tracking system to keep incident records relating to Covered Information, and the ticket owner will record the status, information and solution in the system.

➢ Compliance

TRENDnet has implemented a security audit process to cover internal audit operations related to TRENDnet’s Covered Information security management system and to ensure conformance with TRENDnet’s information security policies, standards, laws and regulations. The nonconforming items will be recorded in the security system audit corrective action report.

• FTC Order Part II - F. Regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures;

TRENDnet’s risk assessment identified the need to build a management process of security testing using both unplanned and periodically scheduled testing as follows:
• FTC Order Part II - G. The development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order, and requiring service providers, by contract, to establish and implement, and thereafter maintain, appropriate safeguards consistent with this order; and

- TRENDSnet has published the “Outsourcing Security Policy”, “Outsourced Product Development” and “Outsourced Service Management” for the management with the business partner.

- TRENDSnet conducts a management process for third party vendors and
business partners.

➢ Application Security Management with Outsourced Service Management

In considering third party applications' security risk, TRENDnet contractually requires partners to follow TRENDnet's “Outsourcing Security Policy” the requirement for Device Functionality development.

➢ Risk management with third party vendors

All third party Device Functionalities are verified for compliance with TRENDnet’s security requirements through outsourcing security testing before integration into the production environment.

➢ Business partners are contractually required to implement and maintain appropriate safeguards and/or agree to meet the requirements in TRENDnet’s Business Partner Information Security Policy. Moreover, all business partners who handle Covered Information are evaluated initially and on an annual basis under a security risk assessment process.

➢ The ISMS Security team has conducted the security review jointly with third party consultant to ensure that policy, security requirements and standards being fulfilled by partners appropriately.

• FTC Order Part II - H. The evaluation and adjustment of the security program in light of the results of the testing and monitoring required by
Subpart F, any material changes to the respondent’s operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its security program.

- The latest threat information is continuously collected from internal forums and external channels as an integral part of the tracking process, in order to respond to new threats.

- All the new security threats will be well classified and evaluated with the risk assessment process and outsourcing security consultant. Following handing of security incident response, TRENDnet will report and record relevant materials providing feedback as lessons learned and make suggestions as to updates to security program including security baseline, information security policy and standard operating procedures.

- The latest system vulnerabilities and attack information are collected and analyzed with outsourcing security consultant in order to update the policy and software guidelines for software development and information security.

- TRENDnet implemented communication structure to ensure that updates regarding security are dispatched to all relevant employees.
5. Summary of First Audit Findings

The first audit was from 19th January, to 21st January, 2015. During the first audit period, the overall assessment with administrative management, implementation of physical and technical controls was examined of the ISO/IEC 27001 standards. Although the basic security framework has been implemented and adopted with documented procedures and safeguards to constitute an effective security program, the first audit showed part of the documented procedures and some practices could be improved. Hence, further review was conducted to confirm compliance with the FTC Order.

The following paragraphs are a brief summary of the first audit:

• Administrative control

  – Issues of Risk identification/Risk assessment/Risk control

  – Issues of Process consistency
6. Summary of Second Audit
7. Conclusion

According to the FTC Order, Part III of the FTC Order requests that TRENDnet, in connection with its compliance with Part II of this Order, shall 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.

III, as an independent third party audit team, conducted the audit to review TRENDnet's implementation of a comprehensive security program for safeguarding TRENDnet's Covered Device, Covered Device Functionality, and Covered Information Systems in compliance with Part II of the FTC Order.

III developed audit objectives based on the requirements of the FTC Order. III also use ISO/IEC 27001:2013 Information technology as the normative reference that implemented within the TRENDnet.

For completeness of assessment, III conducted two audits covering the reporting period of July 1st, 2014 to January 7th, 2015.

In conclusion, after the assessments of reporting period, III hereby certifies that TRENDnet has demonstrated it has implemented a security program that to provide reasonable assurance for the security of Covered Device /Covered Device Functionality and Covered Information in compliance with Part II of the FTC Order.
This assessment includes review of document, administrative, technical, and physical safeguards that TRENDnet has implemented and maintained during the reporting period. TRENDnet also proved the safeguards have been implemented adequately and met the requirements set in Part II of the FTC Order.
8. References


Information security management systems. Requirements. Published by ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission).
9. Appendix

9.1. Appendix A Detail of First Audit Findings
Appendix A  Detail of First Audit Findings

For the purpose of this appendix A, the following terms and definitions apply.

FTC Order shall mean the dedicated items regarding to part II of FTC Order.

Issue type shall mean the types of finding with three categories, ‘Procedure’, ‘Practice’ or ‘Evidence’. Definitions of the categories are listed as below:

• Procedure shall mean the published policy or procedure need to be justified.

• Practice shall mean there were inconsistency existed between operations and the published policy or procedures.

• Evidence shall mean the executing records were not kept in proper formats or demonstrated properly.

• Remediation shall mean the corrective or preventive actions proposed by TRENDnet.

• Status shall mean the different status of finding, the level classified into “open”, “in progress” and “closed”.

Appendix A-1
Table 5 – Audit Findings of TRENDnet

<table>
<thead>
<tr>
<th>FTC Order</th>
<th>Issues Type</th>
<th>Audit Finding</th>
<th>Remediation</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part II.A</td>
<td>Practice</td>
<td>Security team members and their clearly defined responsibilities</td>
<td>Executive management selects team members and defines responsibilities</td>
<td>Closed</td>
</tr>
<tr>
<td>Part II.A</td>
<td>Practice</td>
<td>Develop comprehensive information security policy that encompasses Covered Device, Covered Information, and Covered Information System</td>
<td>Institute for Information Technology (III) developed an enterprise information security policy in conjunction with industry standard ISO 27001:2013</td>
<td>Closed</td>
</tr>
<tr>
<td>Part II.B</td>
<td>Record</td>
<td>Framework to identify and mitigate material internal and external risks to the security of Covered Device</td>
<td>Working with third-party security consultant to develop risk questionnaires and security</td>
<td>Closed</td>
</tr>
<tr>
<td>FTC Order</td>
<td>Issues Type</td>
<td>Audit Finding</td>
<td>Remediation</td>
<td>Status</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>---------------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>test checklists</td>
<td></td>
</tr>
<tr>
<td>Part II.B</td>
<td>Practice</td>
<td>Product vendors to implement reasonable safeguards to mitigate security risks</td>
<td>Request risk assessment results from product vendors and forwarded them to third-party security consultant for further review</td>
<td>Closed</td>
</tr>
<tr>
<td>Part II.C</td>
<td>Practice</td>
<td>Security risk assessment</td>
<td>Risk questionnaires developed by third-party security consultant to ensure proper security risk assessment</td>
<td>Closed</td>
</tr>
<tr>
<td>Part II.C</td>
<td>Procedure</td>
<td>Identification of Covered Information</td>
<td>Developed information asset identification and safeguards</td>
<td>Closed</td>
</tr>
<tr>
<td>Part II.C</td>
<td>Procedure</td>
<td>Documentation ownership and classification</td>
<td>Developed procedure to classify documentation according to its security levels</td>
<td>Closed</td>
</tr>
<tr>
<td>FTC Order</td>
<td>Issues Type</td>
<td>Audit Finding</td>
<td>Remediation</td>
<td>Status</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Part II.C</td>
<td>Practice</td>
<td>Document management and protection</td>
<td>Developed user permissions and document creation/encryption/decryption/destruction policies</td>
<td>Closed</td>
</tr>
<tr>
<td>Part II.D</td>
<td>Procedure</td>
<td>Employee security training programs</td>
<td>Developed additional employee training programs that include computer usage policy, data security policy, laptop security policy, and portable storage device security policy</td>
<td>Closed</td>
</tr>
<tr>
<td>Part II.D</td>
<td>Practice</td>
<td>Security risk associated with product research and development</td>
<td>Working with third-party security consultant, Onward Security, who recommends and performs necessary risk controls</td>
<td>Closed</td>
</tr>
<tr>
<td>Part II.D</td>
<td>Practice</td>
<td>Security report management</td>
<td>Expended collection of security reports from Appendix A-4</td>
<td>Closed</td>
</tr>
<tr>
<td>FTC Order</td>
<td>Issues Type</td>
<td>Audit Finding</td>
<td>Remediation</td>
<td>Status</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>Part II.D</td>
<td>Practice</td>
<td>Risk assessment associated with secure software design and testing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Working with third-party security consultant, Onward security, who conducts unplanned and periodically scheduled security testing with industry standards</td>
<td>Closed</td>
</tr>
<tr>
<td></td>
<td>Part II.D</td>
<td>Practice</td>
<td>Handling of third-party vulnerability reports</td>
<td>Forward reports to product vendors and third-party security consultant for further reviews</td>
</tr>
<tr>
<td></td>
<td>Part II.E</td>
<td>Practice</td>
<td>Security awareness</td>
<td>Enhance information security culture across internal teams through training and</td>
</tr>
</tbody>
</table>

Appendix A-5
<table>
<thead>
<tr>
<th>FTC Order</th>
<th>Issues Type</th>
<th>Audit Finding</th>
<th>Remediation</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part II.E</td>
<td>Practice</td>
<td>Comprehensive information security policy</td>
<td>Adopted ISO 27001:2013 standard</td>
<td>Closed</td>
</tr>
<tr>
<td>Part II.E</td>
<td>Practice</td>
<td>Covered device source code review</td>
<td>Working with third-party security consultant, Onward Security, who conducts source code review</td>
<td>Closed</td>
</tr>
<tr>
<td>Part II.E</td>
<td>Practice</td>
<td>Covered device security testing</td>
<td>Working with third-party security consultant, Onward security, who conducts security testing</td>
<td>Closed</td>
</tr>
<tr>
<td>Part II.E</td>
<td>Practice</td>
<td>Covered device penetration testing</td>
<td>Working with third-party security consultant, Onward security, who conducts security penetration testing</td>
<td>Closed</td>
</tr>
</tbody>
</table>

Appendix A-6
<table>
<thead>
<tr>
<th>FTC Order Issues Type</th>
<th>Audit Finding</th>
<th>Remediation</th>
<th>Status</th>
</tr>
</thead>
</table>

Data Source : III

Appendix A-7