OMB Control Number: 1670-0027
OMB Expiration Date: 01/31/2021

Department of Homeland Security

Cybersecurity and Infrastructure Security Agency (CISA) Partner Satisfaction Survey

The Department of Homeland Security (DHS) Cybersecurity Infrastructure Security Agency (CISA) is charged with enhancing the security, resiliency, and reliability of the nation's cyber, communications, and physical infrastructure, as well as with supporting DHS's mission to manage risk. CISA comprises four divisions: Infrastructure Security Division (ISD), Cybersecurity Division (CSD), Emergency Communications Division (ECD) and National Risk Management Center (NRMC).

To identify opportunities to improve our products and services, we ask that you please take 7 minutes to complete this anonymous and voluntary survey to understand your expectations and values, so we may use the information to help us bring those expectations and values to reality. Thank you.

Please note CISA does not intend to collect any Personally Identifiable Information (PII) such as respondent contact information (names, organizations, phone numbers, email addresses). ***Please do not provide any PII in the open text fields*.**

1. **Which of the following best describes you or your organization/affiliation?**

   a) **Federal Government – DHS (Component or Subcomponent)**
   b) **Federal Government – Not DHS**
   c) **Non-governmental organization**
   d) **Non-profit organization**
   e) **Private Sector and/or Critical Infrastructure**
   f) **Research community/academia**
   g) **State, Local, Territorial, or Tribal government (SLTT)**
   h) **Other (Please identify)**
   Click here to enter text.

2. **What is your current role in your organization?**
   a) **Federal/State/Local/Territorial/Tribal Communications or Public Safety Official**
   b) **Firewall/Intrusion Detection System/Intrusion Prevention System (IDS/IPS) Engineer or equivalent**
   c) **Intelligence Analyst or Intelligence Officer**
   d) **IT Continuity, Contingency, or Disaster Recovery Analyst or equivalent**
   e) **IT Continuity, Contingency, or Disaster Recovery Manager or equivalent**
   f) **IT Project Manager**
   g) **IT Security Analyst or equivalent**
   h) **Malware/Forensic Analyst or equivalent**
   i) **Management Analyst or Program Analyst**
   j) **Manager for IT/Cybersecurity or equivalent**
   k) **Operations Research Analyst**
   l) **Physical Security Analyst or Facility Security Officer**
   m) **Policy Analyst or Strategist**
   n) **President/Vice President/Director/CISO/CIO**
   o) **Quality Assurance Analyst**
   p) **Security Operations Center (SOC) Manager or equivalent**
   q) **SES-level Federal Employee**
   r) **State/Local/Territorial Agency Administrator or Deputy Administrator**
   s) **Other (Please identify)**
      Click here to enter text.

3. **Which <enter ISD, CSD, ECD, NRMC> personnel do you partner with in your current role? (Personnel can be from multiple <enter ISD, CSD, ECD, NRMC> offices; please check all that apply).**
   a) <Enter titles of division personnel>
   b) <Enter titles of division personnel>
   c) <Enter titles of division personnel>
   d) <Enter titles of division personnel>
   e) <Enter titles of division personnel>
   f) <Enter titles of division personnel>
   g) <Enter titles of division personnel>
   h) <Enter titles of division personnel>
   i) <Enter titles of division personnel>
   j) **I am not certain which specific division(s) personnel I partner with, e.g., I only know of a specific POC(s)**

(For Questions 4 to 9): **The Federal Government has directed <enter ISD, CSD, ECD, NRMC>, through various federal directives and**

requirements, to provide <enter cybersecurity or infrastructure or communication or risk management> products and services to organizations. *Please indicate your level of agreement with the following statements regarding* <enter ISD, CSD, ECD, NRMC> *products, services, and information sharing:*

4. **I am satisfied with the *quality* of products and services from <enter ISD, CSD, ECD, NRMC>.**
   a) **Completely agree**
   b) **Somewhat agree**
   c) **Neutral**
   d) **Somewhat disagree**
   e) **Completely disagree**

5. **I am satisfied with the *reliability* of products and services from <enter ISD, CSD, ECD, NRMC>.**
   a) **Completely agree**
   b) **Somewhat agree**
   c) **Neutral**
   d) **Somewhat disagree**
   e) **Completely disagree**

6. **I am satisfied with the *timeliness* of products and services from <enter ISD, CSD, ECD, NRMC>.**
   a) **Completely agree**
   b) **Somewhat agree**
   c) **Neutral**
   d) **Somewhat disagree**
   e) **Completely disagree**

7. **I am satisfied with *how often* <enter ISD, CSD, ECD, NRMC> partners with my organization.**
   a) **Completely agree**
   b) **Somewhat agree**
   c) **Neutral**
   d) **Somewhat disagree**
   e) **Completely disagree**

8. **I am satisfied with how <enter ISD, CSD, ECD, NRMC> *shares information* with my organization.**
   a) **Completely agree**
   b) **Somewhat agree**
   c) **Neutral**
   d) **Somewhat disagree**

e) Completely disagree

9. I find <enter ISD, CSD, ECD, NRMC> products and services *valuable to fulfilling my organization's priorities*.

a) Completely agree
b) Somewhat agree
c) Neutral
d) Somewhat disagree
e) Completely disagree
f) I do not know the value of <enter ISD, CSD, ECD, NRMC> products and services in fulfilling my organization's priorities (Please explain).

Click here to enter text.

10. For what purpose(s) do you use <enter ISD, CSD, ECD, NRMC> products and services in your current role? (Please check all that apply).

a) As indicators and/or alerts, directly in daily operations and system protection
b) Informationally, for internal risk and/or threat analysis efforts
c) Informationally, for assessment and/or performance measurement
d) Informationally, for reporting
e) Operationally, for event and/or incident planning
f) Operationally, for incident response
g) Operationally, for intrusion prevention
h) Operationally, for public safety technical assistance
i) Operationally and/or strategically, to assist in public safety interoperable communications
j) Strategically, for risk and/or threat awareness
k) Strategically, for planning
l) Other (Please explain)

Click here to enter text.

11. In what ways does <enter ISD, CSD, ECD, NRMC> share information with your organization? (Please check all that apply).

a) Direct formal partnership via DHS personnel, e.g., conferences, working groups, workshops, exercises, events, visits, and/or meetings
b) Distributed/printed media
c) Email
d) Phone
e) Information campaigns
f) Website(s) and/or web portal(s) including secure portal(s), e.g., Homeland Security Information Network (HSIN)

g) **Social media platforms**
h) **Webinars**
i) **Other (Please explain)**
Click here to enter text.

12. **How often do you use <enter ISD, CSD, ECD, NRMC> products and services in your current role? Services can include, but are not limited to, <enter ISD, CSD, ECD, NRMC> personnel partnering with your organization to inform its governance, security management, and/or emergency communications planning. (Please select only one answer).**
a) **Daily**
b) **Weekly or bi-weekly**
c) **Monthly**
d) **Periodically, situationally, and/or ad hoc (unpredictable)**
e) **Never, because I am not familiar with <enter ISD, CSD, ECD, NRMC> products and services**
f) **Never, because I do not find <enter ISD, CSD, ECD, NRMC> products and services useful. (Please explain).**
Click here to enter text.

13. **What is the greatest challenge or barrier to partnering with <enter ISD, CSD, ECD, NRMC>? (Please select only one answer).**
a) **Lack of opportunities to actively work with <enter ISD, CSD, ECD, NRMC> to create and/or develop products and services**
b) **Lack of information being shared by <enter ISD, CSD, ECD, NRMC>**
c) **Reporting or other information shared by <enter ISD, CSD, ECD, NRMC> is not timely**
d) **Reporting or other information shared by <enter ISD, CSD, ECD, NRMC> lacks sufficient context**
e) **Lack of knowledge regarding an appropriate <enter ISD, CSD, ECD, NRMC> POC(s) to partner with**
f) **Necessity for a security clearance to access <enter ISD, CSD, ECD, NRMC> products and services**
g) **Lack of an adequate feedback loop for your organization to offer comments and/or suggestions to <enter ISD, CSD, ECD, NRMC> on its products and services**
h) **Time constraints of your organization and/or of <enter ISD, CSD, ECD, NRMC>**
i) **Other (Please explain)**
Click here to enter text.

14. How can your organization benefit more from the products and services <enter ISD, CSD, ECD, NRMC> provides? (Please check all that apply).

a) Reduce impact to your organization when responding to <enter cyber or infrastructure> attacks and other <enter cyber or infrastructure> security incidents
b) Increased networking opportunities
c) Increased and/or more robust information exchanges
d) Greater awareness of <enter cyber or security> risks and/or threats facing your organization
e) Heightened awareness of what <enter ISD, CSD, ECD, NRMC> does
f) Greater ability to put a face with a name in terms of <enter ISD, CSD, ECD, NRMC> personnel you interact with
g) Enhanced ability to meet your organization's goals
h) Increased opportunities for providing feedback to <enter ISD, CSD, ECD, NRMC> e.g., in-person, through surveys
i) Other (Please explain)
Click here to enter text.