ENCLOSURE 1

Social Media or Third-Party Site Security Survey/Plan for Survey Monkey

Note: Gray highlighted text identifies the content each program must fill in when completing a plan – please delete highlighting in completed plans

PROGRAM/DIVISION/CENTER or OFFICE: NCEH/ATSDR/DCHI
SITE NAME AND NAME OF CDC PROFILE(S): ATSDR Communication Activities Survey, Survey Monkey

AUTHORIZING OFFICIAL: Alan Parham, DCHI, OA, 770-488-3657

TECHNICAL REPRESENTATIVE: Matt Sones, Public Health Analyst, ATSDR/DCHI, zgi2@cdc.gov, 770-488-0731

ISSO: Brian Nicholson, NCEH/ATSDR/NCEH, fgi5@cdc.gov , 770-488-6447.

1. BUSINESS AND TECHNICAL CONSIDERATIONS.

   a. FUNCTIONAL DESCRIPTION: Survey Monkey is an online survey tool that can be used to design, collect, and analyze feedback from any user that has internet access. Links to surveys can be distributed to participants via email or through a link posted to a web page. Surveys can be designed so that they fulfill the governance requirements necessary for gathering information from respondents. ATSDR will be using Survey Monkey to survey to collect information from community members and stakeholders at sites where the agency is conducting investigations.

   b. BUSINESS JUSTIFICATION: Survey Monkey will allow the NCEH/ATSDR DCHI collect critical feedback from community members and stakeholders on the quality of services and information provided by DCHI. This data will assist DCHI in assessing how well it is communicating critical risk information to communities and how well the division is addressing the needs of community members living at or near sites where investigations are taking place. Lack of access to this service will negatively impact DCHI's ability to evaluate the quality of its products and services and therefore will prevent the agency from better addressing the needs of community members.

   c. TECHNICAL DESCRIPTION: Survey Monkey provides a web-based interface for design, collecting, and analyzing user feedback. The service requires the establishment of a user account to use the features of the service. Survey participants are not required to have an account to access a survey. Surveys can be designed so that no user information such as email or IP addresses is collected.

   d. INFORMATION TYPES: Based on NIST SP 800-60 analysis, this site's categorization is LOW, based on use of the following information types:

Information Types & Impact Levels[1]

Information Type	NIST SP 800-60 R1 Reference	Confidentiality	Integrity	Availability	Justification for Enhanced Control
Customer Services	C.2.6.1	N/A*	Low	Low	*The information disseminated by this 3rd party site has no confidentiality associated with it and is cleared for public release. The net confidentiality rating for this activity is N/A.
Official Information Dissemination	C.2.6.2	N/A*	Low	Low	
Product Outreach	C.2.6.3	N/A*	Low	Low	
Public Relations	C.2.6.4	N/A*	Low	Low	
OVERALL RATINGS		**NA**	**Low**	**Low**	

*Note: data posted to social media or third-party sites must have a security categorization of **NA for Confidentiality** (all public information) and no greater than LOW impact for Integrity and Availability. Therefore, social media or third-party sites cannot be used for communicating, storing or processing Personally Identifiable Information (PII), information that is otherwise deemed sensitive or protected, including but not limited to Personal Health Information (PHI), financial information, or Controlled Unclassified Information.*

e. All content posted to this site will be approved for public release through one or more of the following processes:
   (1) Authorized CDC channels for scientific information;
   (2) Authorized CDC channels for public communications;
   (3) Other: please specify if applicable

2. RISK CONSIDERATIONS.

a. GENERAL. The CDC program officials listed above are implementing the safeguards described in Tab A to meet CDC and HHS policies, as well as safeguard CDC information, information systems, and/or the public and professional reputation of CDC.

b. SPECIFIC DESCRIPTION AND MITIGATION OF RISKS. The table below elaborates on risks identified with using the particular site, profiles, technologies and/or data involved, and how that risk will be reduced. The table clearly specifies any deviations/adjustments from the safeguards in Tab A.

Risk Area A: CDC External			
#	Risk Description	Background/History	Risk Reduction Controls

[1] If necessary, additional rows may be added to this table.

1	Public/Partner (site user) privacy	The Survey Monkey site is coded in ASP.NET 2.0, running on SQL Server 2008, Ubuntu Linux, and Windows 2008 Server. The Survey Monkey privacy policy is available on the vendor's website.	• Application of the following safeguards listed in Tab A: 3 through 15 • Other: ATSDR (Matt Sones) will utilize the Survey Monkey option that allows survey authors to disable the storage of email addresses and disable IP address collection for all collection methods so that they can collect anonymous survey responses.
2	Public/Partner (site user) exposure to malware or other online threats	Survey Monkey's website security statement states that the site is firewall restricted access to all ports except 80 and 443; Survey Monkey uses intrusion detection systems, conducts QualysGuard network security audits weekly, and conducts McAfee SECURE scans daily.	• Application of the following safeguards listed in Tab A:6, 9, 11, 12 • The external stakeholders who will complete the survey will only be provided to a direct link to the survey.
3	Embarrassment to / penalties against (legal, financial, etc.) CDC		• Application of the following safeguards listed above: 2, 3, 7 through 19 • ATSDR (Matt Sones) is operating within the terms of service agreement issued by HHS for the use of Survey Monkey for this survey. • http://www.hhs.gov/web/socialmedia/policies/tos.html
Risk Area B: CDC Internal Systems			
#	Risk Description	Background/History	Risk Reduction Controls
1	Exposure to malware or other online threats during site administration	Survey Monkey's website security statement states that the site is firewall restricted access to all ports except 80 and 443; Survey Monkey uses intrusion detection systems, conducts QualysGuard network security audits weekly, and conducts McAfee SECURE scans daily..	• Application of the following safeguards listed in Tab A: 6 through 12 • ATSDR (Matt Sones) will only administer the website within the terms and conditions of the safeguards outlined in the site security plan.
Risk Area C: CDC Internal Information			

#	Risk Description	Background/History	Risk Reduction Controls
1	Loss of information due to technical reasons (malicious or operational)		• Application of the following safeguards listed in Tab A: 5 through 7, 11, 12, 15, 16 • No PII will be present in the surveys
2	Loss of information due to administrative or procedural reasons		• Application of the following safeguards listed in Tab A: 2 through 5, 16 • No PII will be present in the surveys to CDC.

c. RISK AREA REFERENCE LINKS (to "Background/History" references above)

1) https://www.mcafeesecure.com/RatingVerify?ref=surveymonkey.com
2) http://clicktoverify.truste.com/pvr.php?page=validate&url=www.surveymonkey.com&sealid=102
3) http://www.surveymonkey.com/privacypolicy.aspx
4) http://help.surveymonkey.com/app/answers/detail/a_id/335/related/1
5) http://www.surveymonkey.com/mp/policy/security/
6) http://www.surveymonkey.com/termsofuse.aspx

3. RISK ACCEPTANCE.

The representative of the coordinating office must circle the appropriate concurrence statement, then write their name, initials and the date to the right. All comments should be captured below the concurrence block or attached as a separate sheet--include the commenter's name and the date. The signed plan must then be forwarded to the supporting ISSO for his/her concurrence. The program maintaining the social media/third-party site must also retain a copy of this concurrence, along with all supporting documents (such as the Terms of Service and Privacy Policy). A completed copy of this document must be scanned and emailed to the OCISO Policy and Planning Team (OCOO-OCISOPolicyandPlanningTeam@cdc.gov) for review.

				NAME and Digital Signature
Program Official	**X** Concur	Concur w/Comment	Non-concur	Matthew Sones -S Digitally signed by Matthew Sones -S Date: 2020.06.10 14:57:36 -04'00'
ISSO	**X** Concur	Concur w/Comment	Non-concur	Brian Nicholson -S Digitally signed by Brian Nicholson -S Date: 2020.06.10 11:53:47 -04'00'

TAB A (Safeguards) to ENCLOSURE 1

1. Use of the site has been coordinated with the CDC Social Media Council and the Office of the Assistant Director / Division of News and Electronic Media (OADC/DNEM), applying CDC best practices.

2. Use of the site and application of appropriate information security and privacy controls have been coordinated with the supporting ISSO.

3. Based on NIST SP 800-60 analysis, this site's categorization is LOW based on identified information types (see paragraph 1d of the survey/plan). *Note: Data posted to social media or third-party sites must have a security categorization of **NA** for Confidentiality (all public information) and no greater than **LOW** impact for Integrity and Availability. Therefore, social media or third-party sites cannot be used for communicating, storing or processing Personally Identifiable Information (PII), information that is otherwise deemed sensitive or protected, including but not limited to Personal Health Information (PHI), financial information, or Controlled Unclassified Information.*

4. All content posted to this site will be approved for public release through one or more of the following processes:
   a. Authorized CDC channels for scientific information;
   b. Authorized CDC channels for public communications;
   c. Other: *see paragraph 1e of the Social Media or Third-Party Site Security Survey/Plan, if applicable*.

5. The program has site-specific Rules of Behavior (RoB) for personnel who administer the site (e.g., create, maintain, access and store site content). Each person reads and acknowledges the RoB.

6. Program personnel administering the site acknowledge and follow the CDC prohibited use policy and *HHS/CDC Rules of Behavior* (RoB) in relation to the programs activities on the site. See the CDC policy, *Use of CDC Information Technology Resources* (CDC-GA-2005-02).

7. The program administers the site using a computer with a current machine image approved by ITSO and meets CDC configuration standards.

8. The program uses passwords meeting CDC standards for all site access, maintenance included.

9. The program applies the *CDC Secure Web Application Coding Guidelines* for any applications used on the site.

10. The program posts a comment moderation policy/statement is posted on the site (if applicable).

11. The program conducts content reviews of its presence on the site at least weekly, checking the following integrity, availability and confidentiality issues.

a. Content: updating or editing outdated, inaccurate, offensive, or otherwise inappropriate content.
b. Security: look for defacements and/or vulnerabilities embedded in site content
c. See Appendix F of DNEM's *Social Media Security Mitigations* for additional guidance.

12. The program has an incident response plan for the site that covers the following (in accordance with CDC incident response standards):
    a. What constitutes an incident;
    b. The offices and individuals to whom an incident is reported and within what timeframe (including the program's ISSO and CDC CSIRT); and
    c. How the responders (program, ISSO, CSIRT) resolve an incident.

13. The program constrains or controls web tracking technology (e.g., cookies) as required by OMB, HHS and CDC policies.

14. The program uses appropriate constraints or controls regarding privacy as required by OMB, HHS and CDC policies, including:
    a. Documenting the review and acceptability of the site's privacy policy (initial, then periodically after use begins);
    b. A Privacy Impact Assessment (PIA), if required;
    c. Posting the CDC/HHS privacy rules and requirements within the program's presence on the site, where appropriate; and
    d. Meeting SORN requirements, if applicable.

15. The program has a signed Terms of Service (TOS) agreement for use of the site that meet HHS guidance. GSA guidance and the CDC Office of the General Counsel (OGC) are consulted as required.

16. The program maintains all information posted to, or downloaded from (if allowed), the site as required by the appropriate Records Schedule/Records Management processes (as determined by the program in consultation with their Senior Records Liaison).

17. The program posts disclaimers on the profile for the site, stating that official CDC information can be found at CDC.gov and that in the case of any discrepancies that the content on CDC.gov be considered correct. CDC's presence should also provide an alternative government email address where users can send feedback.

18. The program uses appropriate CDC branding on the site to distinguish the agency's activities from those of non-government actors.

19. The program posts an alert on links from an official CDC site to any external site.

TAB B (References) to ENCLOSURE 1

OMB

- M-11-02, Sharing Data While Protecting Privacy
- M-10-23, Guidance for Agency Use of Third-Party Websites and Applications
- M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies
- M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information

GSA

- http://www.gsa.gov/graphics/staffoffices/socialmediahandbook.pdf
- http://www.apps.gov

NARA

- http://www.archives.gov/social-media/

HHS CIO COUNCIL

- http://www.cio.gov/Documents/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf
- HHS - OCIO Policy for Information Systems Security and Privacy (HHS-OCISO-2011-0003)
- HHS CIO Policy on Social Media Technologies (HHS-OCIO-2010-0003)
- Updated Departmental Standard for the Definition of Sensitive Information dated May 18, 2009
- HHS-OCIO Memorandum: Implementation of OMB M-10-22 and M-10-23
- HHS Center for New Media – Terms of Service Agreements

CDC

- CDC Enterprise Social Media Policy (CDC-GA-2011-01)
- Use of CDC Information Technology Resources (CDC-GA-2005-02)
- Controlled Unclassified Information (CDC-IS-2005-02)
- Records Management Policy (CDC-GA-2005-07)
- Wireless Security (CDC-IS-2005-01)
- CDC Enterprise Blogging Policy (CDC-GA-2008-03)
- Clearance of Information Products Distributed Outside CDC for Public Use (CDC-GA-2005-06)
- Employee Communication Branding (CDC-CM-2007-01)
- Protection of Information Resources (CDC-IS-2002-06)
- CDC IT Security Program Implementation Standards
- CDC Implementation of the HHS Rules of Behavior
- Division of News and Electronic Media / Electronic Media Branch website
- CDC Social Media Council website
- http://www.cdc.gov/SocialMedia/
- http://www.cdc.gov/SocialMedia/Tools/guidelines/
- http://www.cdc.gov/SocialMedia/Tools/guidelines/pdf/securitymitigations.pdf
- ~~FDCC or SBC (if non-Windows) for workstation used to administer the site off-network~~