OCISO Social Media or Third-Party Site Security Survey/Plan

PROGRAM/DIVISION/CENTER or OFFICE: NCBDDD

SITE NAME AND NAME OF CDC PROFILE(S): *Survey Money*

PROGRAM OFFICIAL: Jason Bonander, Director, NCCDPHP/OD/OIIRM, zjz2@cdc.gov, 770-488-5606

TECHNICAL REPRESENTATIVE: Christopher Pleasants, ORISE Evaluation Fellow, NCBDDD/DCDD/PRTB, ylj0@cdc.gov, 404-498-3871

ISSO: Cindy Allen, NCCDPHP/OD/OIIRM, cdl1@cdc.gov, 770-488-5388

1. BUSINESS AND TECHNICAL CONSIDERATIONS.

   a) FUNCTIONAL DESCRIPTION (what will the site provide the public/partners?): SurveyMonkey will be used to gain insights into the experience of customers who made bulk orders for material from the *Learn the Signs. Act Early. (LTSAE)* program.

   b) BUSINESS JUSTIFICATION (why does CDC need to use this medium/technology to achieve its mission? What is the impact if CDC does not use it?): Improving agency programs requires ongoing assessment of service delivery, a systematic review of the operation of a program compared to a set of explicit or implicit standards, as a means of contributing to the continuous improvement of the program. If this information is not collected, vital feedback from customers on LTSAE's bulk order process will be unavailable.

   c) TECHNICAL DESCRIPTION (what functionality does the site use?): Survey monkey is an online survey platform that captures information from a select group of people. It has functionality to produce skip patterns to reduce burden on respondents and is a well-known as an efficient way to collect information.

   a. 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
General Purpose Data and Statistics	D.20.2	LOW	LOW	LOW	
OVERALL RATINGS		**LOW**	**LOW**	**LOW**	

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

*Note: data posted to social media or third-party sites must have a security categorization of **Not Applicable (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, Sensitive But Unclassified, or Controlled Unclassified Information.*

b. All content posted to the site must be approved for public release through authorized CDC channels and meet OADC Public Communications guidance. Specifically, scientific information must meet Clearance of Information Products Disseminated Outside CDC for Public Use policy.
(1) Other authorized release channel: 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	Public/Partner (site user) privacy	Survey will not contain or collect PII	• Application of the following safeguards listed in Tab A: 3 through 15 • Other: _____
2	Public/Partner (site user) exposure to malware or other online threats	Qualys conducts weekly security scans of the Survey Monkey network.	• Application of the following safeguards listed in Tab A:6, 9, 11, 12 • Other: _____
3	Embarrassment to / penalties against (legal, financial, etc.) CDC	CDC risks implying a relationship with Survey Monkey. CDC could share in backlash if the third party site experienced any security problems.	• Application of the following safeguards listed in Tab A: 2, 3, 7 through 19 • Other: _____
Risk Area B: CDC Internal Systems			
#	Risk Description	Background/History	Risk Reduction Controls
1	Exposure to malware or other online threats during site administration	CDC will administer the survey from within the CDC network. CDC will not have elevated access to SurveyMonkey.	• Application of the following safeguards listed in Tab A: 6 through 12 • Other: _____

2	Exposure to malware by downloading data from the site to CDC networks (only if required)	Consolidated reports will be downloaded from SurveyMonkey and scanned as necessary.	• Use of OCISO-approved USB encrypted drives with malware detection capability • Specific CDC computers or shares where the data will be downloaded, stored, and processed • Detailed procedures/protections used
Risk Area C: CDC Internal Information			
#	Risk Description	Background/History	Risk Reduction Controls
1	Loss of information due to technical reasons (malicious or operational)	Results will be downloaded frequently to avoid loss of information.	• Application of the following safeguards listed in Tab A: 5 through 7, 11, 12, 15, 16 • Other: _____
2	Loss of information due to administrative or procedural reasons	Results will be downloaded frequently to avoid loss of information.	• Application of the following safeguards listed in Tab A: 2 through 5, 16 • Other: _____

c. RISK AREA REFERENCE LINKS (to "Background/History" references above)
Survey Monkey Security Statement:
https://www.surveymonkey.com/mp/policy/security/

3) RISK ACCEPTANCE.

The representative of the coordinating office must circle the appropriate concurrence statement, then sign (electronic signature preferred) and date their name 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 OCISOThirdParty@cdc.gov *for review.*

TAB A (Safeguards)

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 **Not Applicable (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, Sensitive But Unclassified, or Controlled Unclassified Information.*

4. All content posted to the site must be approved for public release through authorized CDC channels and meet OADC Public Communications guidance. Specifically, scientific information must meet Clearance of Information Products Disseminated Outside CDC for Public Use policy. (*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. Digitalgov.gov and OADC 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)

U.S. Office of Government Ethics

- 5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch

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

NIST

- NIST SP 800-60 Rev 1, Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I
- NIST SP 800-60 Rev 1, Guide for Mapping Types of Information and Information Systems to Security Categories, Volume II

GSA

- Digitalgov.gov Negotiated Terms of Service Agreements

NARA

- Social Media and Digital Engagement at the National Archives

HHS CIO COUNCIL

- Privacy Best Practices for Social Media
- HHS Information Systems Security and Privacy Policy (IS2P) – July 2014 Edition
- HHS CIO Memorandum, Usage of Unauthorized External Information Systems to Conduct Department Business
- HHS-OCIO Policy for Managing the Use of Third-Party Websites and Applications
- HHS CIO Memorandum, Updated Departmental Standard for the Definition of Sensitive Information
- HHS CIO Memorandum, Implementation of OMB M-10-22 and M-10-23
- HHS.gov Social Media Terms of Service Agreements

CDC

- CDC Enterprise Social Media Policy
- Use of CDC Information Technology Resources
- Controlled Unclassified Information
- Records Management
- Wireless Security
- CDC Enterprise Blogging Policy
- Clearance of Information Products Distributed Outside CDC for Public Use
- Employee Communication Branding
- Protection of Information Resources
- CDC IT Security Program Implementation Standards
- CDC Implementation of the HHS Rules of Behavior for Use of HHS Information Technology Resources
- Office of the Associate Director for Communication
- OADC Division of Public Affairs
- CDC Social Media Council
- CDC Social Media Tools, Guidelines & Best Practices
- Social Media Security Mitigations
- Standard Baseline Configurations
- OCISO Social Media & Third-Party Websites

05/16/2016

PROGRAM/DIVISION/CENTER or OFFICE: NCBDDD

SITE NAME AND NAME OF CDC PROFILE(S): *Survey Money*

PROGRAM OFFICIAL: Jason Bonander, Director, NCCDPHP/OD/OIIRM, zjz2@cdc.gov, 770-488-5606

TECHNICAL REPRESENTATIVE: Christopher Pleasants, ORISE Evaluation Fellow, NCBDDD/DCDD/PRTB, ylj0@cdc.gov, 404-498-3871

ISSO: Cindy Allen, NCCDPHP/OD/OIIRM, cdl1@cdc.gov, 770-488-5388

Position	Choice 1	Choice 2	Choice 3	Signature and Date
Program Official	☑ Concur	☐ Concur w/Comment	☐ Non-concur	Jason C. Bonander -S Digitally signed by Jason C. Bonander -S DN: c=US, o=U.S. Government, ou=HHS, ou=CDC, ou=People, 0.9.2342.19200300.100.1.1=1001715926, cn=Jason C. Bonander -S Date: 2016.07.15 11:25:12 -04'00'
ISSO	☑ Concur	☐ Concur w/Comment	☐ Non-concur	Cynthia Allen -S Digitally signed by Cynthia Allen -S DN: c=US, o=U.S. Government, ou=HHS, ou=CDC, ou=People, cn=Cynthia Allen -S, 0.9.2342.19200300.100.1.1=1000144116 Date: 2016.07.15 11:05:19 -04'00'