U.S. Department of Health and Human Services

Centers for Disease Control and Prevention

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

Submitted to CISO

DHHS/CDC/OCOO/OCIO/OCISO
4770 Buford Highway, F-35
Atlanta, GA 30341

Approved:_____

Cheri L. Gatland-Lightner

Chief Information Security Officer

Date:_____

CDC
CENTERS FOR DISEASE CONTROL AND PREVENTION

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

VERSION Control

Date	Author/Editor	Version	Notes
06/21/2018	K. Carter	0.1	
07/02/2018	C. Frazier	1.0	

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

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: OSTLTS
SITE NAME AND NAME OF CDC PROFILE(S): _Qualtrics – PHHS Block Grant Assessment
PROGRAM OFFICIAL: Bobbie Erlwein, Branch Chief, rxe5@cdc.gov, 404.498.0262
TECHNICAL REPRESENTATIVES: Cassandra Frazier, Health Scientist, bkx9@cdc.gov, 404.498.0581
ISSO: Kerey Carter, OCISO, kvc2@cdc.gov, 770.488.8674

1. BUSINESS AND TECHNICAL CONSIDERATIONS.

   a. FUNCTIONAL DESCRIPTION (what will the site provide the public/partners?):
   The PHHS Block Grant evaluation team will use Qualtrics for its PHHS Block Grant Assessment. The purpose of the assessment is to assess select cross-cutting outputs and outcomes of the Preventive Health and Health Services Block Grant and demonstrates the utility of the grant on a national level. Qualtrics will enable the PHHS Block Grant Evaluation Team to create a web-based survey with advanced controls and logic and distribute the survey.

   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?):

   The PHHS Block Grant evaluation eeam (PBGET) will use Qualtrics' robust functionality to program and distribute a survey designed to capture data tailored to each respondent. Specific functions include advanced logic, such as incorporating skip logic into qualitative matrices, response validatation, multi-select responses and narrative. PBGET will also use Qualtrics to increase response validity and accuracy by enabling its feature that allows respondents to download and review responses prior to finalizing and submitting the survey.

   Used for the initial PHHS Block Grant Assessment conducted in Fall 2017 (genIC Preventive Health and Health Services Block Grant Assessment OMB No: 0920-0879 Exp. 03/31/2018), Qualtrics has demonstrated its ability to handle a technically complex web-based survey. If PBGET discontinues the use of Qualtrics for this assessment, it will delay or potentially prevent the impelemtation of the survey. PBGET will need to identify a new platform that offers the same level functionality, which could increase cost and delay the implementation of the survey. If PBGET does not identify an equally robust platform, then the assessment would need to be canceled. As a result, PBGET will be unable to assess outputs and outcomes associated with the grant or demonstrate the utility of the grant.

   c. TECHNICAL DESCRIPTION (what functionality does the site use?):

   Qualtrics allows its customers to create and customize online surveys with numerous options during the survey build process. Customers can allow respondents to use custom branding and styles/logos, use web services (such as to link information from RSS feeds or dynamically change a survey's questions or answer choices), send email alerts, create dynamic panels, set response quotas, translate questions into other languages, upload files, and export data to Excel and SPSS. The survey distribution functionality includes the ability to create in-webpage pop-ups, use advanced logic to determine which survey questions respondents see, real-time reporting dashboards, and allows the printing and saving of surveys in Word and PDF formats. The survey report functionality allows customers to create graphs and tables, summary statistics, perform analyses (such as cross tabulations and conjoint analysis). According to the Qualtrics website, the survey solution has SAS 70 Certification and meets Health Insurance Portability and Accountability Act (HIPAA) privacy

standards. The Qualtrics website also states that Qualtrics deploys the general requirements set forth by many Federal Acts, including FISMA. The website provides real-time data replication.

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
Management Improvement	C.2.3.7	N/A*	Low	Low	The data collected under this information type is not linked (directly or indirectly) to any individuals, and the non-identified survey responses in isolation do not reveal confidential information. Therefore, the confidentiality rating is N/A.
OVERALL RATINGS		**N/A**	**Low**	**Low**	

*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.*

e. 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.

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.

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

Risk Area A: CDC External			
#	Risk Description	Background/History	Risk Reduction Controls
1	Public/Partner (site user) privacy	Qualtrics advertises that the company provides a protective privacy policy regarding email addresses and personal information. Personally-identifiable information should not be collected or maintained in any CDC surveys created using the service.	• Application of the following safeguards listed in Tab A: 3 through 15 • OSTLTS will not collect any personally identifiable information within its survey. • Qualtrics adheres to safeguards in TAB A:3-15 • Qualtrics provides a protective privacy policy statement at https://www.qualtrics.com/privacy-statement • Qualtrics complies with the U.S. and E.U. Safe Harbor Framework and the U.S.and Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce
2	Public/Partner (site user) exposure to malware or other online threats	The Qualtrics website may be exposed to malicious content or infections. CDC survey responders could be exposed to malware that can infect local workstations.	• Application of the following safeguards listed in Tab A:6, 9, 11, 12 • The Qualtrics service adhere to safeguards in Tab A:6, 9, 11 • Qualtrics provides a security statement at https://www.qualtrics.com/security-statement. Qualtrics has SAS 70 Certification and meets HIPAA standards. • Qualtrics routinely undergoes monthly patch updates.

• 3	• Embarrassment to / penalties against (legal, financial, etc.) CDC	CDC survey responders may provide incorrect or misleading responses. Incorrect survey results may damage the reputation of the agency or compromise the integrity of the project.	• Application of the following safeguards listed in Tab A: 2, 3, 7 through 19 • The Qualtrics service adheres to Tab A: 2, 3, 7-19 and poses no embarrassment to/penalties against the agency. • Qualtrics has certified that it adheres to the Safe Harbor Privacy Principles
Risk Area B: CDC Internal Systems			
• #	Risk Description	Background/History	Risk Reduction Controls
• 1	• Exposure to malware or other online threats during site administration	While conducting survey administration on the Qualtrics website, CDC staff could be redirected to a malicious website that can compromise the user's workstation.	• Application of the following safeguards listed in Tab A: 6 through 12 • CDC users will use USGB compliant workstations with enterprise virus protection installed using the up-to-date virus/malware/spyware signatures. • Software adhere to safeguards in Tab A:6 – 12 • Qualtrics provides a security statement at https://www.qualtrics.com/security-statement. Qualtrics has SAS 70 Certification and meets HIPAA standards. • Qualtrics routinely undergoes monthly patch updates.

			• Qualtrics provides an acceptable use statement at https://www.qualtrics.com/acceptable-use-statement. Qualtrics states that the company website has a zero tolerance policy for spam, pornography, and warez (pirated software). Any surveys found to contain, promote, or link to such content are subject to immediate removal from the Qualtrics service. •
• 2	• Exposure to malware by downloading data from the site to CDC networks (only if required)	While conducting survey administration on the Qualtrics website, CDC staff could be redirected to a malicious website that can compromise the user's workstation.	• 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 • CDC users will use USGB compliant workstations with enterprise virus protection installed using the up-to-date virus/malware/spyware signatures. • Qualtrics supports ethical research data collection by using secure, encrypted storage under US-EU Safe Harbor Principles. Qualtrics Security Statement: http://www.qualtrics.com/security-statement **NOTE:** See links referenced in section 2C.
Risk Area C: CDC Internal Information			

#	Risk Description	Background/History	Risk Reduction Controls
1	Loss of information due to technical reasons (malicious or operational)	No sensitive data or PII will be present in the surveys. Loss of information does not pose a confidentiality, integrity, or availability risk to CDC.	Application of the following safeguards listed in Tab A: 5 through 7, 11, 12, 15, 16 Qualtrics supports ethical research data collection by using secure, encrypted storage under US-EU Safe Harbor Principles
2	Loss of information due to administrative or procedural reasons	No sensitive data or PII will be present in the surveys. Loss of information does not pose a confidentiality, integrity, or availability risk to CDC.	Application of the following safeguards listed in Tab A: 2 through 5, 16

c. RISK AREA REFERENCE LINKS (to "Background/History" references above)
   1) Qualtrics -- http://www.qualtrics.com/
   2) Qualtrics Survey Software: Handbook for Research Professionals -- http://cloudfront.qualtrics.com/q1/wp-content/uploads/2012/02/QualtricsSurveySoftware.pdf
   3) Qualtrics Security Statement: http://www.qualtrics.com/security-statement
   4) Qualtrics Privacy Statement: https://www.qualtrics.com/privacy-statement
   5) U.S.-EU & U.S.-Swiss Safe Harbor Frameworks: http://export.gov/safeharbor/

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

Position	Choice 1	Choice 2	Choice 3	Signature and Date
Program Official	☒ Concur	☐ Concur w/Comment	☐ Non-concur	7/23/2018 X Program Official Signed by: Roberta K. Erlwein -S
ISSO	☐ Concur	☒ Concur w/Comment	☐ Non-concur	7/23/2018 X Kerey Carter ISSO Signed by: Kerey L. Carter -S

ISSO Comments:

- Qualtrics recently received a FedRAMP accreditation (10/31/2017). Per prior agreement from OCISO, OCISO plans to evaluate the use of Qualtrics at the enterprise level, as multiple CDC offices currently use Qualtrics under approved 3rd party site plans. If OCISO re-evaluates Qualtrics use at CDC and later requires a security assessment and accreditation, OSTLTS understands that this change can circumvent or impact the 3rd party site plan approval.