



PandemicOversight.gov
PRIVACY IMPACT ASSESSMENT
SPENDING INFORMATION

The mission of the Pandemic Response Accountability Committee (the PRAC) is to serve the American public by promoting transparency and conducting and supporting oversight of the coronavirus funding and the Federal government's coronavirus response to prevent and detect fraud, waste, abuse, and mismanagement and to identify and mitigate major risks that cross program and agency boundaries. The PRAC is a committee of the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

This Privacy Impact Assessment is a public document and will be made available to the general public via [PandemicOversight.gov](https://www.pandemicoversight.gov). The previous URL for this site was [Pandemic.Oversight.gov](https://www.pandemicoversight.gov), which will continue to be active as a redirect.

The PRAC - Privacy Impact Assessments (PIA):

[https://www.pandemicoversight.gov/\[ADD APPROPRIATE LINK\]](https://www.pandemicoversight.gov/[ADD APPROPRIATE LINK])

Name of System: PandemicOversight.gov

Document Version: 1.0

Document Date: August 19, 2020

GENERAL INFORMATION:

One of the purposes of PandemicOversight.gov is to provide the public with free access to data on funding under the Coronavirus Aid, Relief, and Economic Security Act, Public Law 116-136, (CARES Act) and other pandemic related legislation, in a user-friendly website to foster greater accountability and transparency of the government's pandemic response and the use of such funds. The creation of this site is mandated by the CARES Act, which requires the site to display certain specified data elements including data on federal awards. Because the jurisdiction of the PRAC does not cover payments to individuals, the website cannot display nor allow searches of such information.

DATA IN THE SYSTEM:

For its transparency mission, the system will import spending data (including awards and subawards) collected by other federal agencies. The primary source for this data will be USASpending.gov, a public website that is operated by the U.S. Department of the Treasury, Bureau of Fiscal Service. The data will be imported into PandemicOversight.gov through USASpending.gov public APIs. This data is reported into USASpending from other federal agencies pursuant to the Digital Accountability and Transparency Act of 2014 and from other systems including the Federal Procurement Data System and the System for Award Management pursuant to the Federal Funding Accountability and Transparency Act of 2006. The data sources are federal agencies and recipients of awards and subawards. Only publicly releasable data is made available through USASpending's APIs.

We expect that the system will also import other spending data (including awards and subawards) collected from recipients of awards and subawards by other federal agencies for pandemic programs, including 1) the U.S. Department of the Treasury Office of Inspector General related to the Coronavirus Relief Fund, 2) the U.S. Department of Health and Human Services related to the Provider Relief Fund (currently displayed on a public website, and 3) the Small Business Administration related to the Paycheck Protection Program (for which awards over \$150,000 are publicly displayed), 4) other federal agencies involved in handling or distributing ~~related to~~ coronavirus funds.

We have reviewed and rely upon the Privacy Impact Assessments (PIAs) or other privacy analyses conducted by the federal agencies from which we will receive the original data. None have required a System of Record Notice for the data that would be transferred to the PRAC.

ATTRIBUTES OF THE DATA:

The use of the data is relevant and necessary for the PRAC's compliance with the CARES Act as noted above. The data elements for USASpending are described in detail in the USASpending database dictionary documentation. The data elements for the Coronavirus Relief Fund are described in detail in the Recipient Reporting Data Dictionary. The Paycheck Protection Program has a data dictionary and

spreadsheet with data variables defined. THHS's PIA that covers the Provider Relief Fund discusses viewable data elements.

Data validation techniques are used to check for accuracy and completeness of the some of the elements of the USASpending data when the data is reported into USASpending; those elements tend to focus on format, character length and other features. Ultimate accuracy and completeness of the data is the responsibility of the submitting agencies. In similar fashion, data validation of some aspects of the Coronavirus Relief Fund will take place when the recipients report into the reporting portal. Ultimately, the recipients are responsible for the accuracy and completeness of the data they submit into the portal. HHS has developed a data quality tool to check for these attributes for the Provider Relief data as set forth in its PIA. The PPP data is dependent on the recipient's willingness to provide relevant, timely and accurate data as set forth in the relevant SBA PIA.

Data updates will be imported from USASpending.gov on a basis that is at least monthly but may be more frequent. Data updates related to the Coronavirus Relief Fund will be imported quarterly. Data updates from other federal agencies will be scheduled to match the reporting cadence.

ACCESS TO DATA:

PandemicOversight.gov provides the public with free on-line access to spending data related to the CARES Act and other coronavirus legislation. In addition to the public, systems administrators, PRAC staff, and contractors working on behalf of the PRAC will have access to the data in the system.

The system in which the data is housed will implement Role-Based Security; roles which will be granted privileges within the system platform will be defined in accordance with PRAC and NIST requirements. System users will be assigned roles utilizing the least-privilege model. Multi-Factor Authentication will be enabled for all privileged users in accordance with NIST and PRAC requirements. Security controls will be implemented to provide a robust capability centered around compliance, incident management, root cause analysis, and continuous monitoring.

The security categorizations are as follows: confidentiality (LOW Impact), integrity (MODERATE Impact), and availability (MODERATE Impact).

The information collected will be kept and disposed of in accordance with the records requirements established by the National Archives and Records Administration.

The mission of the Pandemic Response Accountability Committee (the PRAC) is to serve the American public by promoting transparency and conducting and supporting oversight of the coronavirus funding and the Federal government's coronavirus response to prevent and detect fraud, waste, abuse, and mismanagement and to identify and mitigate major risks that cross program and agency boundaries. The PRAC is a committee of the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

This Privacy Impact Assessment is a public document and will be made available to the general public via [PandemicOversight.gov](https://www.pandemicoversight.gov). The previous URL for this site was [Pandemic.Oversight.gov](https://www.Pandemic.Oversight.gov), which will continue to be active as a redirect.

The PRAC - Privacy Impact Assessments (PIA):

[https://www.pandemicoversight.gov/\[ADD APPROPRIATE LINK\]](https://www.pandemicoversight.gov/[ADD APPROPRIATE LINK])



PANDEMICOVERSIGHT.GOV
PRIVACY IMPACT ASSESSMENT

Name of System: PandemicOversight.gov

Document Version: 1.0

Document Date: August 19, 2020

GENERAL INFORMATION:

One of the purposes of PandemicOversight.gov is to provide the public with a means for confidential reporting of fraud, waste, or abuse or criminal activity related to the pandemic funding or the pandemic response as provided for in the Coronavirus Aid, Relief, and Economic Security Act, Public Law 116-136, (CARES Act). The website will function as a portal for the complaints. The complainant will complete a fillable form that the website will transmit through a secure relay to an email box that is outside the system. That information will be reviewed by subject matter experts who will sort the complaints for referrals to other investigative organizations or for other action. No complaint information will be stored in this system.

DATA IN THE SYSTEM:

The source of all data in the system is the complaint reporting process described above. The individuals who may be identified by the incoming complaints include the following: individuals making an allegation of wrongdoing related to the coronavirus spending or pandemic response; the subjects or potential subjects of allegations of wrongdoing; and individuals may simply be requesting information. However, none of this information will be stored in the system.

ATTRIBUTES OF THE DATA:

The use of the data is relevant and necessary for the PRAC's compliance with the CARES Act as noted above. The data elements are contained on the form that is filled out by complainants or requestors of information.

Data collected through complaint reporting will be verified for accuracy and completeness during the course of any investigation or audit performed by the organization to which the allegation is referred. That organization will take appropriate steps to independently verify information produced through the use of independent inquiry to resolve any discrepancies or inconsistencies with the source data provided. Data collected through the hotline reporting will be updated as needed during the course of any investigation or audit performed by the organization to which the complaint is referred.

ACCESS TO DATA:

Systems administrators and contractors working on behalf of the PRAC will have access to the data in the system.

The system in which the data is housed will implement Role-Based Security; roles which will be granted privileges within the system platform will be defined in accordance with PRAC and NIST requirements. System users will be assigned roles utilizing the least-privilege model. Multi-Factor Authentication will be enabled for all privileged users in accordance with NIST and PRAC requirements. Security controls will

be implemented to provide a robust capability centered around compliance, incident management, root cause analysis, and continuous monitoring.

The security categorizations are as follows: confidentiality (MODERATE Impact), integrity (MODERATE Impact), and availability (MODERATE Impact).

The information collected will be kept and disposed of in accordance with the records requirements established by the National Archives and Records Administration.