
**Federal Trade Commission**
**Privacy Impact Assessment**

# Conference Room Scheduling PIA

**July 2014**

## 1. System Overview

The Federal Trade Commission (FTC) uses conference spaces in various FTC facilities and FTC-leased facilities for public-facing events, internal FTC activities, and meetings with external parties. To better coordinate and schedule these activities, the FTC uses an online scheduling system, which integrates with the FTC's existing Microsoft Outlook application. The online scheduling system, which runs on the FTC network and is only accessible to authorized FTC employees and contractors, allows users to schedule conferences and meetings; reserve FTC conference spaces; and generate requests for media equipment and event support, including room set-up.

For activities held at the FTC's Constitution Center, the online scheduling system also pushes out information for display on digital signs. To avoid the unnecessary disclosure of personally identifiable information (PII), the Constitution Center digital signs will only display the name of the meeting owner, the meeting owner's FTC contact information if given (e.g., FTC extension number), and the meeting time; the names or contact information for other attendees will not be displayed on Constitution Center digital signs. To avoid inadvertent display of nonpublic information, the Constitution Center digital signs are configured to prevent a meeting title or other information from Outlook or the scheduling system from being displayed. By default, meeting titles (regardless of sensitivity) in Outlook will be replaced on the Constitution Center digital signs with the generic title, "Private Meeting," and that default meeting description can only be altered by the FTC event planner.

The online scheduling system allows authorized system administrators to generate a variety of reports for statistical purposes, including number of events in a specific period of time, types of event (e.g., non-public vs. public, catered vs. non-catered), maximum room capacity, media equipment required, etc. The online scheduling system is accessed from an icon in Microsoft Outlook, and, together with Outlook, permits FTC meeting organizers to schedule events and send meeting requests to FTC employees, contractors, and external invitees.

## 2. Information Collected and Stored within the System

The following questions are intended to define the scope of the information in the online scheduling system, specifically the nature of the information and the sources from which it is obtained.

### a. What information is to be collected, used, disseminated, or maintained by the system?

The online scheduling system can collect the following information: location (conference room number or name), meeting or event title (as designated by the meeting organizer), room setup, floor plan, any specialized requirements, timing (setup time, dry-run time, begin date/time, end date/time), information about

meeting attendees and participants (number of attendees, whether they are FTC only or FTC and external, whether security or other specialized handling is needed), and media coverage and any related needs (e.g., print and/or camera press coverage, press table, etc.).

To reserve space for an FTC event at the shared conference rooms at Constitution Center, the FTC event planner extracts the necessary event information from the online scheduling system and provides it to the Constitution Center building management.

For activities at the FTC's Constitution Center, the online scheduling system provides limited information for use on digital signs, but that information is limited to the name of the meeting owner, the meeting owner's FTC contact information if given (e.g., FTC extension number), the meeting time, and the default meeting title of "Private Meeting," which can only be altered by the FTC event planner.

For events at the shared conference rooms at Constitution Center, the only personal information collected by the system will be the name and FTC contact information of the FTC event planner.

Outlook calendar invitations regarding the event are separate from the online scheduling system, and that information is handled in accordance with the Data Center General Support System (GSS) PIA.[1]

**b. What are the sources of the information in the system?**

Authorized FTC employees and contractors with FTC network access submit event information (See Section 2a for list of potential data elements submitted) directly via Outlook and the integrated online scheduling system.

The FTC's event planner will submit information to the Constitution Center property manager for events hosted at the shared conference space.

**c. Why is the information being collected, used, disseminated, or maintained?**

The information is collected and used to set up meetings, monitor room usage, track "no show" meetings, and measure room and equipment utilization for space planning and equipment purchases.

**d. How is the information collected?**

FTC employees or contractors who have FTC network access manually enter information (See Section 2a) into Outlook and the integrated online scheduling system.

[1] For current FTC PIAs, see http://www ftc.gov/site-information/privacy-policy/privacy-impact-assessments.

For shared conference room spaces at Constitution Center, the FTC event planner collects information from the online scheduling system and provides the minimum information necessary to the Constitution Center property manager. No PII other than the event planner's name and FTC contact information is provided to the Constitution Center building management, and the event title does not disclose nonpublic information.

**e. How will the information be checked for accuracy and timeliness (currency)?**

All FTC employees coordinating meetings are required to enter accurate information into the online scheduling system at the time of entry, and they also have the ability to edit their entries for accuracy after submission to the event planner. The event planner, as an authorized system administrator, has the ability to correct entries for accuracy and timeliness. Additionally, authorized system administrators within the Office of Chief Information Officer (OCIO) have the ability to review access logs should a question arise about changes to entries.

**f. Is the system using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?**

Yes. The online scheduling system is a new technology used in conjunction with the FTC's existing Outlook application. For activities held at the FTC's Constitution Center, the online scheduling system also pushes out meeting information for display on digital signs, which is a new technology for the FTC. To avoid the unnecessary disclosure of personally identifiable information (PII), the Constitution Center digital signs will only display the name of the meeting owner, the meeting owner's FTC contact information if given (e.g., FTC extension number), and the meeting time; the names or contact information for other attendees will not be displayed on Constitution Center digital signs. To avoid inadvertent display of nonpublic information, the Constitution Center digital signs are configured to prevent a meeting title or other information from Outlook or the scheduling system from being displayed. By default, meeting titles (regardless of sensitivity) from Outlook will be replaced on the Constitution Center digital signs with the generic title, "Private Meeting," and that default meeting description can only be altered by the FTC event planner.

Because only authorized users with FTC network access can view this information and the underlying information in Outlook, this system should not further affect individuals' privacy beyond, as discussed in Section 2.a, disclosing meeting organizer and invitees names and contact information via Outlook schedulers and displaying the name and contact information of meeting organizers on Constitution Center digital signs.

For meetings in the Constitution Center common areas, the FTC event planner will not submit attendees' names, meeting title, or subject matter information to the Constitution Center property manager.

**g. What law or regulation permits the collection of this information?**

The collection of documents and information is authorized by the Federal Trade Commission Act, 15 U.S.C. §§ 41-58.

**h. Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?**

There is a potential privacy risk that nonpublic information such as a meeting's topic and personal information in the form of names of attendees could be inadvertently disclosed or displayed to third parties, via the system itself or via Constitution Center digital signs. To mitigate this risk, only authorized FTC staff and contractors are granted access to the network, Outlook, and the scheduling function. Access to the Outlook calendar and scheduling information, depends on a particular user's role and responsibilities, consistent with the FTC's least privilege access practices. In addition, as discussed in Section 2f, the default displays on Constitution Center digital signs will show the minimum information necessary, and only authorized system administrators can change the default display after review to make sure that no PII or nonpublic information will be disclosed.

For activities in the shared Constitution Center space, only the FTC event planner will share the minimum information with the property manager. The event planner will only submit the minimum information necessary for an event in the Constitution Center auditorium or other shared space. The FTC event planner's name and contact information will be the only personal information submitted to the Constitution Center property manager, and the event will only be described as one involving the FTC. The remainder of the information submitted will be event set-up and logistics.

## 3. Use and Access to Data in the System

The following questions are intended to clearly describe how the information in the system will be used, and who will use it.

**a. Describe how information in the system will or may be used.**

The information in the online scheduling system will be used to schedule meetings in conjunction with Outlook and provide information about set-up and logistics for FTC events, conferences, and general Agency meetings. The information may also be used to compile statistical reports to allow the event

coordinator to track events, equipment, and similar meeting metrics, in a given day, week, or month.

**b. Which internal entities will have access to the information?**

All authorized FTC network users can schedule meetings through Outlook and the integrated online scheduling system. Access to information about specific meetings will depend on the following roles:

System administrator – An OCIO employee will act as the technical system administrator and will resolve technical issues with the online scheduling system. Some members of the Administrative Services Office (ASO) will also share this role from the perspective of managing the users and maintaining the system. The system administrators will have full access to the online scheduling system and related Outlook functionality, and all such access will be logged.

Event planner – FTC administrative staff who will handle the day-to-day room scheduling, generate reports, and coordinate event set-up and logistics. The event planners will have the authority to access, view, create, modify, and delete meetings, forms, and reports and also to change default information displayed on digital signs at Constitution Center.

Meeting owner – FTC staff who initiates an event in Outlook and the online scheduling system. The meeting owners have the authority to create, modify, and delete meetings that they have initiated.

Meeting attendee – FTC staff and third parties who can view Outlook schedulers for meetings that they have been invited to. Meeting attendees will also be able to view digital signs located outside conference rooms at Constitution Center.

**c. Which external entities will have access to the information?**

For the online scheduling system, individuals who received an email invitation from the FTC can view the information, and any descriptions (subject matter, location, date, and time) that the meeting owner has included in the Outlook scheduling email. Third parties will not have access to the online scheduling system.

In addition, third parties (invitees and visitors) may see event information on the digital signs at Constitution Center, but they cannot access or change that information.

## 4. Notice and Access for Individuals

The following questions are directed at how or whether the individual is notified of the scope of information collected. They also concern the individual's right to consent to

uses of information, right to decline to provide information, ability to ensure the accuracy of the information collected, and right to access their information.

**a. How will individuals be informed about what information is collected, and how this information is used and disclosed?**

Individuals receive notice about the FTC's collection, use, and disclosure of their personal information through the FTC's privacy policy.[2] Because the information used in the online scheduling system comes from Outlook and from the FTC user scheduling the meeting, there is no formal communication to individuals about the information collected at the time of meeting creation. Information about how the FTC uses personal information collected through the online scheduling system is described within this document and in the FTC's privacy policy located at: www.ftc.gov/ftc/privacy.shtm.

**b. Do individuals have the opportunity and/or right to decline to provide information?**

No, as to FTC employees and contractors who use Outlook and the online scheduling system. Note that the only personal information contained in the online scheduling system will be FTC contact and event planner information.

Yes, as to invitees and visitors. Invitees can accept invitations to, attend, or decline to attend events to which they are invited. Visitors attending public events may decide that they do not wish to provide their first or last name, or show an approved form of Government-issued photo identification upon arrival at FTC facilities; however, without this information, the FTC cannot confirm the identity of the individual and cannot grant him or her access to the building or to a meeting as required.

**c. Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?**

No, as to FTC employees and contractors who use Outlook and the online scheduling system. No other formal channel currently exists other than to simply decline access to the system and the associated active directory.

No as to invitees and visitors. As noted in 4.b, invitees and visitors can only decline to attend or decline to provide personal information sufficient to permit building access; they cannot limit use of that information except to the extent stated in the FTC's privacy policy, located at: www.ftc.gov/ftc/privacy.shtm

Note that the FTC will not use the scheduling system to retrieve information by personal identifiers except as to FTC organizers.

[2] http://www.ftc.gov/site-information/privacy-policy/privacy-impact-assessments

**d. What are the procedures that allow individuals to gain access to their own information?**

FTC employees, FTC contractors, and external parties with a meeting invitation from Outlook can view the invitation. Individuals can obtain access to their own information by submitting a Privacy Act request to the FTC's FOIA Office. See FTC's FOIA page at: http://www.ftc.gov/about-ftc/foia/foia-request.

**e. Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.**

Because of the limited nature of the data collection and the lack of direct access to the system by external parties, very little risk exists in providing individuals access to their own records.

## 5. Web Site Privacy Issues

Complete this section only if the new system or project creates or modifies an FTC Web site, page, or online form accessible through the Internet.

**a. Describe any tracking technology used by the Web site and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, Web beacon). Currently, persistent tracking technology is not approved for use by the FTC (see 5.2).**

Not applicable. The scheduling system resides on the FTC's Intranet and is not a website accessible to third parties. As to authorized FTC users and contractors, the scheduling system does not have persistent or temporary tracking technologies.

**b. If a persistent tracking technology is used, ensure that the proper issues are addressed (issues outlined in the FTC's PIA guide).**

Not applicable.

**c. If personal information is collected through a Web site, page, or online form accessible through the Internet, is appropriate encryption used? If not, explain.**

Not applicable.

**d. Explain how the public will be notified of the Privacy Policy.**

Not applicable.

**e. Considering any Web site or Internet issues, please describe any privacy risks identified and how they have been mitigated.**

Not applicable.

**f. If the Web site will collect personal information from children under 13, or be directed at such children, explain how it will comply with the Children's Online Privacy Protection Act (COPPA).**

Not applicable.

## 6. Security of Information in the System

The following questions are intended to describe technical safeguards and security measures.

**a. Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?**

The FTC follows all applicable Federal Information Security Management Act (FISMA) requirements. The FTC network, which hosts Outlook, the online scheduling system**,** and the digital signs at Constitution Center, is categorized and authorized to handle moderate risk information as defined using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

**b. Has a Certification & Accreditation been completed for the system or systems supporting the program?**

Yes. The software is accredited as part of the Data Center GSS.

**c. Has a risk assessment been conducted on the system?**

Yes.

**d. Does the project employ technology that may raise privacy concerns? If so, please discuss its implementation.**

The conference room scheduling software allows FTC users with network access to create meetings on any topic with participants who are internal, external, or both. For the online scheduling system, information is maintained in Outlook, which is accessible only to authorized FTC employees or FTC contractors. The only information that external parties may view is the meeting name, attendee email contact information, and information about the subject matter of the meeting, as contained in the scheduler email.

In addition, as discussed in Section 2.f, the default displays on Constitution Center digital signs will show the minimum information necessary, and only authorized system administrators can change the default display after review to make sure that no PII or nonpublic information will be disclosed.

**e. What procedures are in place to determine which users may access the system and are they documented?**

All FTC positions are assigned a risk designation and associated personnel screening criteria. All potential FTC employees, contractors, and volunteers are subject to background investigations and suitability reviews per OMB guidance. Before any new employee, contractor, or volunteer can access any data in Outlook (which includes the online scheduling system and Constitution Center digital signs**),** they must first attend new employee orientation and successfully complete FTC's Privacy and Security Awareness training. There are procedures to address access restrictions for higher-risk employees such as interns and International Fellows.

**f. Describe what privacy training is provided to users either generally or specifically relevant to the program or system.**

All FTC employees and designated contractor personnel with network access are required to complete computer security training and privacy awareness training annually. Interactive online training covers topics such as how to properly handle PII and other data, online threats, social engineering, and the physical security of documents.

FTC employees and contractors with significant security responsibilities are required to undergo additional, specialized training, tailored to their respective responsibilities.

**g. What auditing measures and technical safeguards are in place to prevent the misuse of data?**

Auditing measures and technical safeguards are in place commensurate with the National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems and Organizations Moderate-Impact Baseline Special Publication (SP) 800-53, rev 4.

**h. To whom should questions regarding the security of the system be addressed?**

Any questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer.

## 7. Data Retention

This section addresses for how long data is maintained, and how and when it is disposed.

**a. For what period of time will data collected by this system be maintained?**

The FTC will maintain and dispose of PII and other information collected through online scheduling system in accordance with FTC regulations, policies, and procedures, and with FTC records retention schedule N1-122-09-1 approved by the National Archives and Records Administration (NARA).

**b. What are the plans for destruction or disposal of the information?**

All data will be securely disposed of in accordance with OMB, NARA, and NIST regulations and guidelines and with FTC policies and procedures.

**c. Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.**

See Section 2h. regarding privacy risks identified in data retention and how those risks have been mitigated. The data will be disposed of in accordance with OMB, NARA, and NIST regulations and guidelines and with FTC policies and procedures.

## 8. Privacy Act

This section addresses the applicability of the Privacy Act of 1974 to the system, and whether or not the system is covered by a System of Records Notice (mandated for some systems by the Privacy Act of 1974).

**a. Will the data in the system be retrieved by a personal identifier?**

Yes as to FTC meeting organizers, but not as to meeting attendees. Because data in the online scheduling system and Constitution Center digital signs can be retrieved by the meeting organizer's name and email address, system data can be retrieved by a personal identifier.

**b. Is the system covered by an existing Privacy Act System of Records notice (SORN)?**

Yes. For the online scheduling system and for the Constitution Center digital signs, the applicable SORN is VII-3 -- *Computer Systems User Identification and Access Records -- FTC* (for login credentials of system administrators).

## 9. Privacy Policy

This section confirms that the information handling practices of the system are consistent with the FTC's privacy policy.

**a. Confirm that the collection, use, and disclosure of the information in this system has been reviewed to ensure consistency with the FTC's privacy policy.**

Yes, the collection, use, and disclosure of information in this system are consistent with the FTC's Privacy Policy, which can be found at http://www.ftc.gov/site-information/privacy-policy.

## 10. Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____
Darlene Lyles
Support Services Supervisor

Review:

_____ Date: _____
Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____
Peter B. Miller
Chief Privacy Officer

_____ Date: _____
Jeffrey Smith
Chief Information Security Officer

_____ Date:_____
Jeffrey Nakrin
Director, Records and Filings Office

Approved:

_____ Date:_____
Bajinder Paul
Chief Information Officer