

For Official Use Only

NGSS Privacy Impact Assessment



# NCPC General Support System (NGSS) Privacy Impact Assessment

*Security Categorization: Moderate*

---

VERSION 1.0

AUGUST 19, 2015

Office of Administration NATIONAL CAPITAL PLANNING COMMISSION  
| WASHINGTON, DC

## Document Revision History

Version	Date	Summary of Changes	Author
0.1	October 14, 2014	Initial Draft	Knowledge Consulting Group (KCG)
0.2	November 5, 2014	Incorporate client comments/responses	KCG
0.3	November 17, 2014	Recovery File	NCPC
0.4	December 1, 2014	Removed duplicate 'Process' sections in the privacy analysis Completed the privacy analysis for all privacy areas.	NCPC
0.5	December 10, 2014	Incorporated comments from Deborah Young	NCPC
1.0	August 19, 2015	Signature by SAOP and PO	NCPC

Prepared for:

NATIONAL CAPITAL PLANNING COMMISSION

(NCPC)

401 9th St., NW Suite 500

Washington, DC 20004

By

Knowledge Consulting Group (KCG)

2000 Edmund Halley Drive, Suite 500

Reston, VA 20191

NGSS Privacy Impact Assessment

For Official Use Only (FOUO)

## Abstract

The Office of Administration (OA) is developing the National Capital Planning Commission (NCPC) General Support System (NGSS) Privacy Impact Assessment (PIA). NGSS is used throughout NCPC providing a means of data transport for NCPC users. NGSS provides unclassified but sensitive network services including: local area network (LAN), file servers, application servers (for e-mail, web development, office automation [i.e. as electronic mail, word processing, spreadsheets, electronic forms, databases and specialized financial applications]), desktop workstations, portable devices and associated communications to support all personnel at NCPC with computing services.

A Privacy Threshold Analysis (PTA) was performed and it was determined that NGSS collects, maintains, and/or shares Personally Identifiable Information (PII). Therefore this system requires the development of a PIA.

## References and Guidance

The following documents were referenced for the creation of this standard:

- NCPC Information Security Policy, December 2013
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- OMB Memorandum 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

### Summary Information

<b>Date Submitted for Review</b>	November 17, 2014
<b>System Name</b>	NCPC General Support System (NGSS)
<b>System Owner</b>	Deborah Young
Email	deborah.young@ncpc.gov
Phone Number	202-482-7228
<b>Authorizing Official</b>	Barry Socks
Email	barry.socks@ncpc.gov
Phone Number	202-482-7209
<b>Information System Security Officer</b>	Grace M. Kim
Email	grace.kim@ncpc.gov
Phone	202-482-7214

## Overview

NGSS is a general purpose, multi-user system used throughout NCPC providing a means of data transport for NCPC users. NGSS provides sensitive but unclassified network services including: local area network (LAN), file servers, application servers (for web development and office automation [i.e. as electronic mail, word processing, spreadsheets, electronic forms, databases and specialized financial applications]), desktop workstations, portable devices and associated communications to support all personnel at NCPC with computing services.

The servers, workstations, applications, and network devices are managed and operated by the Office of Administration (OA) at the NCPC office in Washington, DC. The network components provide users with access to application servers, data storage areas, file transfer capabilities, video conferencing capabilities, voice and external data communications.

The users of NGSS are internal NCPC employees, contractors and guests. The Public<sup>1</sup> are not considered users because they can only access the Public Web Services (PWS) server which is outside the authorization boundary. But it is noted that PII belonging to public registrants and provided through the web interfaced is stored in NGSS databases.

Internet connectivity is provided by NCPC's Managed Trusted Internet Protocol Service (MTIPS) provider, CenturyLink. CenturyLink also manages, operates, and monitors the network boundary protection devices, including the security firewall, security (border) router, and network switches. Access from the internet to NGSS is limited to the remote access secure gateway. There is no dial-in access to NGSS via a Remote Access Server (RAS). Remote access is performed via a Fortinet FortiGate Virtual Private Network (VPN) which utilizes Windows authentication to the network.

---

<sup>1</sup> NCPC encourages public participation in the monthly Commission meetings. The meetings are open to the Public and individuals who would like to speak at meetings must register in advance by providing their name, address, telephone number, email address, company and/or professional affiliation. The registration process is the extent of the Public's use of NGSS.

## Section 1: Authorities and Other Requirements

### 1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The legal authorities for the following categories are as follows:

**1. Personnel and payroll information including employee and contractor name, address, phone number, and social security number (to include records on grievances filed by employees):**

- 40 U.S.C. § 871 I(d) (NCPC's authorizing legislation);
- OPM authorities and employee related authorities contained in Title 5 of the U.S. Code and Title 5 of the Code of Federal Regulations. (Applicable to employees);
- USG authorities on money and finance contained in Title 31 of the U.S. Code; and
- Federal laws and regulations pertaining to procurement especially the Federal Acquisition Regulation (FAR) (Applicable to Contractors).

**2. Information regarding individuals who wish to speak at Commission meetings including name, address, telephone number, e-mail address, company and/or professional affiliations:**

- 40 U.S.C. 8701 et seq, (NCPC's authorizing legislation); Federal laws and regulations requiring public participation such as the Administrative; Procedures Act (5 U.S.C. 553(a)) and the Sunshine Act (5 U.S.C. 552(b));
- Memorandum from Barrack Obama, President of the United States, to Heads of Executive Departments on Agency Transparency and Open Government (January 21,2009);
- Memorandum from Peter R. Orszag, Director of the Office of Management and Budget, to Heads of Executive Departments and Agencies on Open Government Directive (December 8, 2009);
- NCPC Open Government Plan (September 14, 2014); and
- NCPC's Revised Procedures for Public Participation, 48 FR 9095 (March 3, 1983).

**3. Information regarding individuals listed on NCPC's mailing list including name, address and where applicable, the organization, group, and institution represented by the individual.**

- 40 U.S.C. 8701 et seq. (NCPC's authorizing legislation);

NGSS Privacy Impact Assessment

- Federal laws and regulations requiring public participation such as the Administrative Procedures Act (5 U.S.C. 553(a)) and the Sunshine Act (5 U.S.C. 552(b));
- Memorandum from Barrack Obama, President of the United States, to Heads of Executive Departments on Agency Transparency and Open Government (January 21, 2009);
- Memorandum from Peter R. Orszag, Director of the Office of Management and Budget to Heads of Executive Departments and Agencies on Open Government Directive (December 8, 2009); and
- NCPC Open Government Plan (September 14, 2014).

**4. Agency visitor sign-in sheets including name and affiliation:**

- 40 U.S.C. 8701 et seq. (NCPC's authorizing legislation); and
- Federal laws applicable to the General Services Administration (GSA) and the Department of Homeland Security (DHS) and regulations and guidance issued by GSA, DHS and the Interagency Security Committee (ISC) governing workplace security. (e.g., 41 C.F.R. § 102.80).

**1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?**

The NCPC has three SORNs pertaining to the NCPC's mailing lists, personnel/payroll, and grievance records. See, Publication of Proposed Changes to Systems of Records as published at 57 F .Reg. 47881 (copy attached). NCPC recognizes that it needs to undertake a systematic review of its records and determine whether additional SORNs are necessary. It is interesting to note that payroll records are now maintained on the system of the Department of Agriculture, National Finance Center's system such that it appears a SORN for payroll records may be unwarranted.

**1.3 Has a system security plan been completed for the information system(s) supporting the project?**

Yes, the system security plan (SSP) for NGSS, version 05, was updated on November 14, 2014. The current ATO expiration date for NGSS is December 2015. The system is currently undergoing re-assessment and authorization due to changes to the system security categorization.

**1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?**

Yes, NCPC have approved NARA retention schedules. NCPC uses the General Records Schedule for payroll and personnel documents.

**1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in the box below, or attach as an appendix.**

NCPC is in the process of requesting approval from OMB under the PRA to communicate with federal agencies and the public to conduct surveys.

## Section 2: Characterization of the Information

### 2.1 Identify the information the project collects, uses, disseminates, or maintains.

1. Personnel and payroll information including employee and contractor name, address, phone number, and social security number are collected from individuals who are currently employed or contracted by or seeking employment with NCPC.
2. NCPC encourages public participation. Information regarding individuals who wish to speak at Commission meetings including name, address, telephone number, e-mail address, company and/or professional affiliations are collected.
3. NCPC offers information about agency operations and decisions online and makes them readily available to the public. Information regarding individuals listed on NCPC's mailing list including name, address and where applicable, the organization, group, and institution represented by the individual are collected for the purpose of notifying them of the latest NCPC news and updates.
4. Visitors of NCPC must sign-in at the front lobby. Visitors provide their name, business affiliation, NCPC contact, and date and time of entry and exit.

### 2.2 What are the sources of the information and how is the information collected for the project?

This information is collected directly from individuals. Individuals provide their information voluntarily in the following methods:

1. Agency employee/contractor provide personnel-related information on paper forms which HR then inputs into NGSS. Agency employees provide PII via a training request form in electronic or paper form.
2. Guest speakers at monthly commission meeting provide their contact information via email, phone and/or paper format.
3. NCPC offers information about agency operations and decisions online and makes them readily available to the public. Information regarding individuals listed on NCPC's mailing list including name, address and where applicable, the organization, group, and institution represented by the individual are collected for the purpose of notifying them of the latest NCPC news and updates.
4. Agency visitors provide their name, professional affiliation, reason for visit, badge number, escort name, and when they entered and exited the NCPC suite.

**2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.**

No, the NGSS does not use information from commercial sources or publicly available data. Information is provided directly from the individual.

**2.4 Discuss how accuracy of the data is ensured.**

Automated controls are not in place to verify the accuracy of the data entered; however, the recipient of the data manually inspects the information to ensure the information is complete.

**2.5 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.**

**Privacy Risks**

The use of the collected data in NGSS is both relevant and necessary to the performance of the Agency's mission. In all cases the program collects information directly from the individual.

Policies and procedures to ensure that personally identifiable information is accurate, complete, and current are not formally documented.

**Mitigations**

NCPC is in the process of developing and documenting a Privacy Program Plan that will address policies and procedures to ensure personally identifiable information is accurate, complete, and current.

NCPC personnel are required to complete privacy awareness training which address privacy handling requirements and privacy incident reporting. Privacy awareness training is completed upon hiring and annually thereafter. This ensures that any misuse or improper access to data is met with sanctions and accountability.

## Section 3: Uses of the Information

### 3.1 Describe how and why the project uses the information.

1. Personnel and payroll information including employee and contractor name, address, phone number, and social security number are collected from individuals who are currently employed or contracted by or seeking employment with NCPC. Information is collected directly from employees or potential employees on forms and through electronic and paper means for the purpose of performing Human Resource operations.
2. Information regarding individuals who wish to speak at Commission meetings including name, address, telephone number, e-mail address, company and/or professional affiliations are collected. This information is used to notify speakers if the agenda item they are registered to speak on is removed from the agenda. This information is also used to notify these persons of the latest NCPC news and updates.
3. Individuals who would like to sign-up for NCPC news, alerts, and announcements can join the NCPC mailing list by providing their name, address and where applicable, the organization, group, and institution represented by the individual on the NCPC website. The list contains only the information necessary to achieve this purpose as it collects the appropriate contact information to reach interested individuals.
4. Visitors of NCPC must sign-in at the front lobby. Visitors provide their name, business affiliation, NCPC contact, and date and time of entry and exit for physical security controls.

### 3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how the Agency plans to use such results.

Information is stored, but is not manipulated in any way other than to populate address fields for a mass email or paper mailing. Data may be input into electronic spreadsheets and accessed by data elements.

### 3.3 Are there other Offices/Agencies with assigned roles and responsibilities within the system?

No.

**3.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.**

<b>Privacy Risks</b>
<p>The risk presented by the use of information collected by NCPC as described above is that the information would be used in ways outside the scope intended by the initial collection.</p> <p>Individuals who provide their personal information are not formally notified of the potential uses of their information.</p>
<b>Mitigations</b>
<p>NCPC has performed this privacy impact assessment (PIA), which describes the potential uses of privacy information. This PIA is posted on the public website for the public to view. Additionally, all NCPC employees and contractors are trained on the appropriate use of personally identifiable information.</p> <p>Individuals who provide personal information should be notified of the potential uses of their information and they should agree to the terms of uses prior to them providing the information.</p>

**Section 4: Notice**

The following questions seek information about the project’s notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

**4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.**

<p>This privacy impact assessment and the System or Records Notice provide notice regarding the collection of information by NCPC.</p> <p>The Privacy Act Statement provides individuals with notice of the voluntary nature of the collection and authority to collect the information.</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project/data collection?**

NCPC will use the information only for the purposes for which it was collected. If an individual suspects information is being used beyond the given scope of the collection, they can contact the system owner and/or privacy officer listed in this privacy impact assessment.

1. Personnel and payroll information – In every case, individuals have proactively sought to provide NCPC with PII, whether it is for existing or prospective employment. Any right to decline to provide information is exercised when choosing to be employed or seek employment with NCPC.
2. Commission meeting speakers – Speaking at the Commission meeting is voluntary. Individuals who volunteer to speak at a Commission meeting must sign up in advance.
3. NCPC mailing list users – All public data collection is voluntary. Only the following information is required if the individual would like to join the NCPC mailing list – email, first name, and last name.
4. Visitors of NCPC - All public data collection is voluntary. If the individual would like to physically enter the NCPC office, they must provide their personal information for security purposes.

**4.3 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.**

<b>Privacy Risks</b>
Personnel and Payroll Information Information within NGSS comes from the individuals, such as an applicant or employee, to whom it applies or is derived from information the individual supplied. Notice is provided at the original point of collection.  The privacy risk associated with notice in the collection of contact information (e.g., speaker contact information, mailing list information, visitor log information) is that the individual is not aware of the purpose for which the information he or she submits may be used.
<b>Mitigations</b>
This risk is primarily mitigated by limiting the use of contact information to what is necessary for the purposes of contacting the person according to his or her voluntary subscription or request.

## Section 5: Data Retention by the Project

The following questions are intended to outline how long the project retains the information after the initial collection.

### 5.1 Explain how long and for what reason the information is retained.

1. Personnel and Payroll Information – The data will be used to respond to any human resources issues including but not limited to time attendance, recruitment, payroll, Equal Employment Opportunity (EEO) issues or law suits, and disciplinary actions.
2. Commission Speaker – Speaker contact information becomes part of the official meeting records, which are retained in accordance with the General Record Schedule defined for the related project.
3. Contact List – Contact information is retained no longer than is useful for carrying out the information dissemination or collaboration purposes for which it was originally collected. Individuals may request their information be deleted if he or she is no longer interested in receiving information from NCPC, after which point their information will not be retained.
4. Visitor List – In accordance with NARA General Records Schedule 18, *Security and Protective Services Records*, logs used to record names of outside contractors, service personnel, visitors, employees admitted to areas are destroyed two (2) years after date of document.

### 5.2 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

<b>Privacy Risks</b>
The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The retention schedule should align with the stated purpose and mission of the system.
<b>Mitigations</b>
NCPC only retains information necessary for the purpose of supporting the participant transactions. PII is retained only for as long as necessary and relevant to fulfill the business requirements.

## Section 6: Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

### 6.1 Is information shared outside of NCPC as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Personnel and Payroll Information is saved and stored on the NGSS network in a folder accessible only to agency personnel with need-to-know (e.g., Director of Office of Administration and the HR Specialist). Externally, information is input into WebTA and NFC for HR processing. Service Level Agreements are in place with these entities to describe security control implementation.

Speaker information is saved in an electronic spreadsheet that is accessible only to the Office of Secretariat for the purpose of documenting. Speaker information and agency visitor information are not shared with external entities

NCPC utilizes a commercial online marketing service to manage the agency's email marketing and event marketing campaigns. Information collected from individuals who sign-up for the NCPC mailing list will be shared with this commercial entity.

### 6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

**Personnel and Payroll information** – NCPC submits personnel and payroll information in WebTA and NFC.

**Mailing List Information** – There is a SORN for mailing list information which states the purpose is to provide interested individuals information on Commission policies, procedures, and meeting agenda to interested parties and persons. The list contains only the information necessary to achieve this purpose as it collects the appropriate contact information to reach interested individuals. The SORN states information is purged upon request.

**Speaker and Visitor information** – Contact information collected from Commission speakers and visitors are not shared with external entities.

**6.3 Does the project place limitations on re-dissemination?**

NCPC's Interagency Agreement authorizes the National Finance Center (NFC) to release payroll or personnel data in accordance with the provisions of the Freedom of Information Act (FOIA) and the Privacy Act.

**6.4 Describe how the project maintains a record of any disclosures outside of the Department.**

NCPC's current Privacy Regulations do not address this issue. See, 1 C.F.R. § 455 (copy attached). New regulations in the final stages of drafting assign the record keeping function to the Privacy Act Officer. They also establish requirements addressing accounting for disclosures and procedures for responding to a request for an accounting of disclosures.

**6.5 Privacy Impact Analysis: Considering the extent of internal and external information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.**

<b>Privacy Risks</b>
The privacy risk to sharing information with internal and external entities is the disclosure of information.
<b>Mitigations</b>
The system employs role-based security by organization which limits internal sharing of data. Records are maintained in a secured environment with access limited to authorized personnel whose duties require access.  Security controls are in place to protect the transfer of data with external entities. MOUs and SLAs are in place formally documenting roles and responsibilities.

**Section 7: Redress**

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

**7.1 What are the procedures that allow individuals to access their information?**

Per section 455.3 (a), "an individual who wishes to know whether a system of records maintained by the Commission contains a record pertaining to him or her shall submit a written request to that effect to the appropriate System Manager at the Commission. The System Manager shall, within 10 days of the receipt of such submission, inform the individual whether a system of

records maintained by the Commission contains such a record.”

Section 455.3 (b) continues, “An individual who desires access to any identified record shall file a request therefor, addressed to the System Manager indicating whether such individual intends to appear in person at the Commission’s offices or whether he or she desires to receive a copy of any identified record through the mail.”

**7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?**

Per section 455.6 , “an individual may request that a record pertaining to him or her be amended or corrected...”

Section 455.7 of NCPC's current privacy regulations states, “within ten days of the receipt of the request to correct or to amend the record, the System Manager will acknowledge in writing such receipt and promptly either: (a) Make any correction or amendment of any portion thereof which the individual believes is not accurate, relevant, timely, or complete and inform the individual of same; or (b) inform the individual of his or her refusal to correct or to amend the record in accordance with the request, the reason for the refusal, and the procedures established by the Commission for the individual to request a review of that refusal.”

**7.3 How does the project notify individuals about the procedures for correcting their information?**

The following information is contained on the NCPC's website:

The U.S. Department of Justice Office of Information and Privacy provides guidelines for all federal agencies, including the National Capital Planning Commission. This Office has a helpful website

[http://www.usdoj.gov/oip/04\\_7.html](http://www.usdoj.gov/oip/04_7.html) that includes the following guides:

- Your Right to Federal Records: Questions and Answers on the Freedom of Information Act and the Privacy Act (2006) (includes complete text of the law)
- DOJ FOIA Guide (March 2007)
- DOJ Privacy Act overview (May 2004)

Upon adoption, NCPC's new privacy regulations will be contained on the website and the link to the Federal Register publication included as well.

**7.4 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.**

<b>Privacy Risks</b>
The privacy associated with redress is the inability to access and/or correct their information.
<b>Mitigations</b>
<p>Individuals may correct their information at any time during which the Agency possesses and use their contact information.</p> <p>Per section 455.6 , “an individual may request that a record pertaining to him or her be amended or corrected...”</p> <p>Section 455.7 of NCPC's current privacy regulations states, “within ten days of the receipt of the request to correct or to amend the record, the System Manager will acknowledge in writing such receipt and promptly either: (a) Make any correction or amendment of any portion thereof which the individual believes is not accurate, relevant, timely, or complete and inform the individual of same; or (b) inform the individual of his or her refusal to correct or to amend the record in accordance with the request, the reason for the refusal, and the procedures established by the Commission for the individual to request a review of that refusal.”</p>

## Section 8: Auditing and Accountability

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

### 8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

NCPC's Interagency Agreement with NFC states that it conducts a Privacy Impact Assessment (PIA) prior to placing a new system of record in place and every three (3) years thereafter and whenever a significant system change occurs. The PIA analyzes how information is handled and the privacy associated with information systems.

### 8.2 Describe what privacy training is provided to users, either generally or specifically, relevant to the project.

All Department employees and contractors are required to receive annual privacy and security training to ensure their understanding of proper handling and securing of personally identifiable information such as what is contained in contact lists.

### 8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

All personnel, agency employees and contractors, will undergo Background Investigations which will be performed by OPM. The System Owner approves new account access, along with the personnel account's role and privilege level(s) to the degree necessary to carry out their responsibilities. Thereafter, the system administrator provisions the newly authorized user in accordance with system owner approval. Account creation is tracked and logged within the Track-IT ticketing system

### 8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within the NCPC and outside?

NCPC has an Interconnecting System Agreement (ISA) with USDA. This agreement is reviewed every three years or upon significant changes to the agreement. The ISA was last updated in 2014.

## Responsible Officials

Deborah Young, System Owner  
deborah.young@ncpc.gov  
202-482-7228

Barry Socks, Authorizing Official  
barry.socks@ncpc.gov  
202-482-7280

Grace Kim, Information System Security Officer  
grace.kim@ncpc.gov  
202-482-7214

Anne R. Schuyler, General Counsel  
[anne.schuyler@ncpc.gov](mailto:anne.schuyler@ncpc.gov)  
202-482-7223

## Approval Signature Page

// Original Signed //

---

Barry S. Socks  
Senior Agency Official for Privacy  
National Capital Planning Commission

8/19/15

---

Date

// Original Signed //

---

Anne R. Schuyler  
Privacy Officer  
National Capital Planning Commission

8/19/2015

---

Date