



**Privacy Impact Assessment**  
**Facility Security System (On Guard)**  
**Major Application**

*Revision: 1.1*

*USDA OCIO NITC*

*Date: February 2010*



## Document Information

Owner Details	
Name	Greg Schmitz
Contact Number	816-926-2356
E-mail Address	Greg.Schmitz@ocio.usda.gov

Revision History			
Revision	Date	Author	Comments
1	10/24/2008	Brandon Sifford	Initial Version
1.1	11/3/2008	Brandon Sifford	Updated questions 5.1, 5.2, 8, 9.1, 9.2, 20, 21, 23, 29, 29.1 and Section 5 based on feedback from Greg Schmitz.
1.1	02/10/2010	Rob Arentsen	Updated document to delete references to the use of SSNo and to add a second location.

Distribution List			
Name	Title	Agency/Office	Contact Information
Greg Schmitz	Chief, Security Division	USDA-OCIO-NITC 8930 Ward Parkway Kansas City, MO 64114	816-926-2356 Greg.Schmitz@ocio.usda.gov



## Table of Contents

DOCUMENT INFORMATION.....	II
TABLE OF CONTENTS.....	III
1 SYSTEM INFORMATION.....	1
2 DATA INFORMATION.....	3
2.1 Data Collection.....	3
2.2 Data Use.....	4
2.3 Data Retention.....	5
2.4 Data Sharing.....	6
2.5 Data Access.....	6
2.6 Customer Protection.....	7
3 SYSTEM OF RECORD.....	8
4 TECHNOLOGY.....	8
5 COMPLETION INSTRUCTIONS.....	9



# 1 System Information

<b>System Information</b>	
Agency:	USDA-OCIO-NITC
System Name:	Facility Security System (On Guard) Major Application
System Type:	<input checked="" type="checkbox"/> Major Application <input type="checkbox"/> General Support System <input type="checkbox"/> Non-major Application
System Categorization (per FIPS 199):	<input type="checkbox"/> High <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> Low
Description of System:	<p>OnGuard is a security technology integration application suite used to control and manage physical access devices and video surveillance systems at the National Information Technology Center (NITC). The application was developed by Lenel of Pittsford, New York and provides access control, alarm monitoring, digital video, intrusion detection, asset tracking, information security integration, credential production, and employee and visitor management functionality for building tenants at 8930 Ward Parkway and at the Goodfellow Data Center in St. Louis.</p> <p>OnGuard is one of the NITC's Major Applications. The application is owned and managed by the NITC Security Staff and used by security personnel under contract to the General Services Administration and NITC security administrators. System access is limited to these two distinct user groups.</p> <p>The system allows authorized security personnel to grant and monitor multiple entry points at the Ward Parkway and Goodfellow sites simultaneously from one centralized location at each site.</p> <p>The application also provides a platform for viewing real-time or archived video recorded through a network of internal and external surveillance cameras. It also provides the management of security badges, including automated verification of issued credentials, and generation and management of new access badges for new and existing employees, authorized visitors, and contractors.</p> <p>The Department of Agriculture, NITC is the sole source input agency for the system.</p> <p>Data in the system include a photograph, the name, worker status (Federal or contractor), and fingerprint data for all workers (both Federal and contracted) and visitors to the two sites. The fingerprint is a digitized configuration of a scanned fingerprint that cannot be recreated to the original fingerprint.</p>
Who owns this system? (Name, agency, contact information)	Greg Schmitz USDA-OCIO-NITC 8930 Ward Parkway Kansas City, MO 64114 816-926-2356 Greg.Schmitz@ocio.usda.gov



Privacy Impact Assessment for Facility Security System (On Guard)

---

Who is the security contact for this system? (Name, agency, contact information)	Greg Schmitz USDA-OCIO-NITC 8930 Ward Parkway Kansas City, MO 64114 816-926-2356 Greg.Schmitz@ocio.usda.gov
Who completed this document? (Name, agency, contact information)	Rob Arentsen USDA-OCIO-NITC 8930 Ward Parkway Kansas City, MO 64114 816-823-1071 rob.arentsen@ocio.usda.gov



## 2 Data Information

### 2.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	<p>The information contains a photograph, the name, worker status (Federal or contractor), and fingerprint date for all workers (both Federal and contracted) and visitors to 8930 Ward Parkway.</p> <p>The fingerprint is a digitized configuration of a scanned fingerprint that can not be recreated to the original fingerprint.</p> <p>However, sensitive information is not transferable in report formats. These elements are not built in to the reporting application capabilities.</p>
2	Does the system collect Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 3.
2.1	State the law or regulation that requires the collection of this information.	N/A – The system does not collect Social Security Numbers (SSN's) or Taxpayer Identification Numbers (TIN's)
3	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
4	Sources of the data in the system.	Information is collected from Federal and contracted workers and visitors.
4.1	What data is being collected from the customer?	Information is not collected from customers
4.2	What USDA agencies are providing data for use in the system?	USDA agencies do not provide data for use in the system.
4.3	What state and local agencies are providing data for use in the system?	State and local agencies do not provide data for use in the system.
4.4	From what other third party sources is data being collected?	Information is collected only from Federal and contracted workers and visitors.
5	Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e., NFC, RD, etc.) or Non-USDA sources.	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 6.
5.1	How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?	N/A – data is not collected from customers, only Federal and contracted workers as well as visitors.
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	N/A – data is not collected from USDA Agencies, only Federal and contracted workers as well as visitors.



No.	Question	Response
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	N/A – data is not collected from non-USDA sources or any other third party sources.

## 2.2 Data Use

No.	Question	Response
6	Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?	Data is used only for Facility Access.
7	Will the data be used for any other purpose?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 8.
7.1	What are the other purposes?	N/A – Data will not be used for any other purpose other than facility access.
8	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
9	Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e., aggregating farm loans by zip codes in which only one farm exists.)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 10.
9.1	Will the new data be placed in the individual's record (customer or employee)?	N/A – no new data will be derived
9.2	Can the system make determinations about customers or employees that would not be possible without the new data?	N/A – no new data will be derived
9.3	How will the new data be verified for relevance and accuracy?	N/A – no new data will be derived
10	Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?	Data is used only for Facility Access.
11	Will the data be used for any other uses (routine or otherwise)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 12.
11.1	What are the other uses?	N/A – data will have no other use.



No.	Question	Response
12	Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 13.
12.1	What controls are in place to protect the data and prevent unauthorized access?	N/A – Data is not being consolidated. The On-Guard system does not interface with other systems and the servers are protected with restricted access within a restricted building.
13	Are processes being consolidated?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 14.
13.1	What controls are in place to protect the data and prevent unauthorized access?	N/A – no processes are being consolidated. The system physically secured and isolated from other systems. NITC has implemented system security controls to protect data and prevent unauthorized access.

### 2.3 Data Retention

No.	Question	Response
14	Is the data periodically purged from the system?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No – If NO, go to question 15.
14.1	How long is the data retained whether it is on paper, electronic, in the system or in a backup?	The data is kept on the system for as long as it is needed. Inactive card holders are deleted from the system. DVR records are deleted after thirty days. Transaction records are archived to file after 180 days. They are stored indefinitely. Backup tapes are overwritten after seven days.
14.2	What are the procedures for purging the data at the end of the retention period?	DVR records, transaction records, and backup tapes are overwritten. There are no regular reports generated. Ad hoc reports are destroyed. Procedures are documented in Security Operating Instructions.
14.3	Where are these procedures documented?	The NITC security office.
15	While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	The Biometric data used does not change. The data is accurate due to the immediate removal of separated employees.
16	Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No



## 2.4 Data Sharing

No.	Question	Response
17	Will other agencies share data or have access to data in this system (i.e., international, federal, state, local, other, etc.)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 18.
17.1	How will the data be used by the other agency?	N/A – Data is not shared.
17.2	Who is responsible for assuring the other agency properly uses the data?	N/A – Data is not shared.
18	Is the data transmitted to another agency or an independent site?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 19.
18.1	Is there appropriate agreement in place to document the interconnection and ensure the PII and/or Privacy Act data is appropriately protected?	N/A – Data is not transmitted.
19	Is the system operated in more than one site?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No – If NO, go to question 20.
19.1	How will consistent use of the system and data be maintained in all sites?	OnGuard systems are located at two sites. The systems at both sites are managed by the same personnel using the same procedures and the same controls.

## 2.5 Data Access

No.	Question	Response
20	Who will have access to the data in the system (i.e., users, managers, system administrators, developers, etc.)?	Physical security staff, guards and system administrators.
21	How will user access to the data be determined?	There are no users outside the security staff, guards and system administrators.
21.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
22	How will user access to the data be restricted?	These systems at both locations are in restricted environments. The database is only accessible on restricted computers within restricted access areas. User ID and Password is required to gain access to data on this stand-alone network.
22.1	Are procedures in place to detect or deter browsing or unauthorized user access?	<input checked="" type="checkbox"/> Yes – User ID and password is required to log into the system. <input type="checkbox"/> No



No.	Question	Response
23	Does the system employ security controls to make information unusable to unauthorized individuals (i.e., encryption, strong authentication procedures, etc.)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No The system resides is on an isolated network and uses authentication to access the interface and database.

## 2.6 Customer Protection

No.	Question	Response
24	Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e., office, person, departmental position, etc.)?	Specific members of the NITC Security Division and guards are responsible for the physical security of the data. This system's interface is only accessible via a isolated network to the above group of staff.
25	How can customers and employees contact the office or person responsible for protecting their privacy rights?	They can contact the Chief, Security Division NITC, listed as the system owner.
26	A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?	<input checked="" type="checkbox"/> Yes – If YES, go to question 27. <input type="checkbox"/> No
26.1	If NO, please enter the Plan of Action and Milestones (POA&M) number with the estimated completion date.	N/A – a "breach" policy is in place.
27	Consider the following: <ul style="list-style-type: none"> <li>▪ Consolidation and linkage of files and systems</li> <li>▪ Derivation of data</li> <li>▪ Accelerated information processing and decision making</li> <li>▪ Use of new technologies</li> </ul> Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 28.
27.1	Explain how this will be mitigated?	N/A – The potential to deprive a customer of due process rights does not exist.
28	How will the system and its use ensure equitable treatment of customers?	Customers are not allowed to have access to this system. This system is in a restricted environment. The database is only accessible on restricted computers within restricted access areas.
29	Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 30



No.	Question	Response
29.1	Explain	This system is designed to allow specific workers into specific locations within the buildings based upon their individual or group job responsibilities. Job responsibilities are the only criteria used to make this determination.

### 3 System of Record

No.	Question	Response
30	Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No – If NO, go to question 31
30.1	How will the data be retrieved? In other words, what is the identifying attribute (i.e., employee number, social security number, etc.)?	Data is not retrieved. Scanned biometric data is compared with stored biometric data, based on an ID badge number.
30.2	Under which Systems of Record (SOR) notice does the system operate? Provide number, name and publication date. (SORs can be viewed at <a href="http://www.access.GPO.gov">www.access.GPO.gov</a> .)	On-Guard operates under systems of records notice E6-15901, <i>Federal Personal Identify Verification Identity Management System</i> . [Federal Register: September 28, 2006 (Volume 71, Number 188)].
30.3	If the system is being modified, will the SOR require amendment or revision?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

### 4 Technology

No.	Question	Response
31	Is the system using technologies in ways not previously employed by the agency (e.g., Caller-ID)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, the questionnaire is complete.
31.1	How does the use of this technology affect customer privacy?	N/A – The use of privacy does not impact the customer privacy.



## 5 Completion Instructions

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c (Is there at least one Privacy Impact Assessment (PIA) which covers this system?) is **Yes**.

PLEASE SUBMIT A COPY TO THE OFFICE OF THE ASSOCIATE CHIEF  
INFORMATION OFFICE FOR CYBER SECURITY.



## Privacy Impact Assessment Authorization

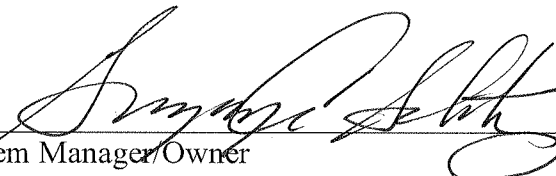
### Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Facility Security System (On Guard)  
(System Name)

This document has been completed in accordance with the requirements of the E-Government Act of 2002.

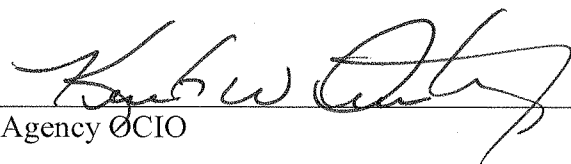
We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

  
\_\_\_\_\_  
System Manager/Owner  
OR Project Representative  
OR Program/Office Head.

3/29/2010  
Date

N/A per Rick Ciampa  
\_\_\_\_\_  
Agency's Chief FOIA officer  
OR Senior Official for Privacy  
OR Designated privacy person

\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Agency OCIO

9/1/2010  
Date

