MAY 1 6 2012

OCIO Directive 2012-007

To: Assistant Directors for Information Resources

Through: Kimberly A. Thorsen
           Deputy Assistant Secretary
           Law Enforcement, Security and Emergency Management

           (For)
           Pamela R. Malam
           Deputy Assistant Secretary
           Human Capital and Diversity

           Andrew Jackson
           Deputy Assistant Secretary
           Technology, Information and Business Services

From: Bernard J. Mazer
           Chief Information Officer

Subject: Guidance for Short-Term State and Local Emergency Response Personnel Regarding
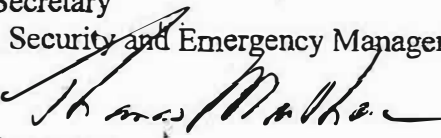   Access to Department Networks and Resources

On February 17, 2012, the United States Department of Agriculture's (USDA) Chief Information
Officer (CIO) and I approved a request to accept risk for granting short-term state and local
emergency response personnel without full background investigations access to USDA and the
Department of the Interior's (DOI) General Support Systems (GSS). As a result, I am rescinding
DOI's Office of the Chief Information Officer (OCIO) Directive 2011-005, and issuing the
following guidance for granting such access. USDA is issuing similar guidance to ensure that
common policies and practices are followed throughout the respective organizations.

This directive applies to the Wildland Fire program activities in the following DOI
organizations:

- Office of the Secretary;
- Bureau of Land Management;
- Bureau of Indian Affairs;
- National Park Service; and
- Fish and Wildlife Service.

This directive grants qualifying short-term state and local emergency response support personnel
access to federal networks and resources without possessing HSPD-12 identity credentials,

including fingerprint checks and/or background investigations. Each of the affected organizations will adhere to the 25 mitigating controls described in the February 17, 2012 Memorandum (Attachment A). Any permanent or temporary entity (for example, a dispatch center or an incident organization) that grants short-term state and local emergency response personnel access to DOI networks without full background investigations will follow these procedures:

- Establish an appropriate number of short-term computer user accounts consisting of predefined login names and passwords, to be assigned to these short-term emergency response personnel. Each issuing office shall document the granting of these short-term accounts.
- Provide all short-term non-federal emergency employees with Rules of Behavior for use of Information Technology (IT) systems for review and signature.
- Conduct and track IT Security Awareness Training as outlined in Attachment A.
- Provide short-term emergency response personnel with IT Security Awareness training as found in Attachment B.
- Establish a Service Level Agreement (SLA) between each dispatch center and the servicing IT organization using the template found in Attachment C. The SLA must be in place prior to establishing the user accounts for short-term emergency response personnel.
- Document any security violations involving these personnel, and immediately report them to the appropriate authority.

Each affected organization is responsible for transmitting this guidance to all affected elements of the organization for implementing the guidance in coordination and collaboration with interagency partners, and for providing appropriate monitoring and oversight. If you have questions regarding this policy, please contact, Chris Rutherford at Christopher_Rutherford@ios.doi.gov or 202-208-5433.
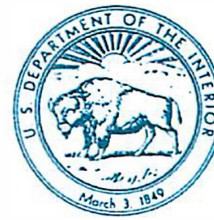
cc: Kirk Rowdabaugh, Director, Office of Wildland Fire

Attachments:

Attachment A - Memorandum of February 17, 2012
Attachment B - Information Technology Security Awareness Training Procedures
Attachment C - Information Technology Security Awareness Training
Attachment D - Service Level Agreement Template

THE DEPARTMENT OF AGRICULTURE   FEB 1 7 2012   **THE DEPARTMENT OF THE INTERIOR**

TO: Bernard J. Mazer
         Chief Information Officer, Department of the Interior

         Christopher L. Smith
         Chief Information Officer, Department of Agriculture

FROM: Kim A. Thorsen
         Deputy Assistant Secretary Law Enforcement, Security and Emergency
         Management, Department of the Interior

         James E. Hubbard
         Deputy Chief, State and Private Forestry, USDA Forest Service

SUBJECT: Risk Acceptance Details for Granting Short-Term State & Local Emergency
         Response Personnel without Full Background Investigations Access to USDA and
         DOI General Support Systems

Background:

Both the Department of the Interior (DOI) and the Department of Agriculture (USDA), through the U.S. Forest Service, routinely use non-federal personnel from state, local, and tribal organizations in emergency response to wildland fires. The integrated response capability of the federal and non-federal wildland fire organizations, made possible by a system of shared, standardized qualifications and incident resource management protocols, is fundamental to our ability as a Nation to respond to emergency fire incidents in an efficient and cost-effective manner. Use of non-federal personnel on wildland fire incidents and in support capacities such as dispatch is an essential component of the business of federal wildland fire management.

Historically these non-federal personnel have been granted logical access to agency systems and networks when such access was inherent to the duties for which they are qualified to perform and the tasks to which they are assigned. However, the provisions of HSPD-12 and other federal policy documents governing access management require federal agencies to conduct background investigations on employees who require logical access to agency systems and networks.

OMB M-05-24 allows agencies to make a risk-based decision for individuals requiring logical access for less than 6 months (aggregate) including guest researchers, volunteers, intermittent, temporary or seasonal employees. Per DOI Personnel Bulletin No. 09-06, the definition of an employee needing logical access includes short term employees (i.e. less than 180 calendar

1

days), detailed or assigned to DOI and all other affiliates such as, but not limited to, guest researchers, volunteers, tribal users, or intermittent and temporary or seasonal employees. Based on this definition of employee, DOI agencies are required to initiate and adjudicate a background investigation on anyone requiring logical access. USDA uses the definition of employee, defined in title 5 U.S.C §2105 and further defined by Executive Order (EO) 12968, to mean a person, other than the President and Vice President, employed by, detailed or assigned to, USDA, including members of the Armed Forces; an expert or consultant to USDA; an industrial or commercial contractor, licensee, certificate holder, or grantee of USDA, including all subcontractors; a personal services contractor; or any other category of person who acts on behalf of an agency as determined by the agency head. In addition, routine access is defines as a person that is accessing the facility and/or information system without an escort and/or continuous monitoring by a USDA official. The agency's determination should be based upon the support to successfully complete USDA's mission critical functions/missions. This type of access requires a mandatory PIV ID credential to be issued.

The logical access provisions of HSPD-12, OMB policy, and policies of the Departments of Agriculture and the Interior significantly inhibit the ability of our wildland fire programs to efficiently, cost-effectively, and safely manage emergency wildland fire incidents. This decision document lays out the justification for a risk acceptance activity for allowing the wildland fire programs of DOI and USDA to access federal networks and resources without requiring a background investigation, with use of the mitigating controls that both organizations have already put in place to reduce the risk involved to meet this business need.

Decision Point:

We believe it is in the best interest of both USDA and DOI to accept the risk for certain short-term state and local emergency response support personnel to access these federal networks and resources without requiring a background investigation.

Business Value:

The interagency firefighting community is made up of the USDA Forest Service; four DOI bureaus: Bureau of Land Management (BLM), National Park Service (NPS), Bureau of Indian Affairs (BIA), and the Fish and Wildlife Service (FWS); State forestry agencies through the National Association of State Foresters and Tribes. Combined, these organizations form the National Wildfire Coordinating Group (NWCG). The purpose of NWCG is to coordinate programs of the participating wildfire management organizations to avoid wasteful duplication and provide a means of constructively working together. Its goal is to provide more effective execution of each organization's fire management program. The group provides a formalized system to agree upon standards of training, equipment, workforce qualifications, and other operational functions.

The NWCG has the following creed:

- *We believe the goal of effective wildfire management is best served through coordinating the resources of all fire management agencies, irrespective of land jurisdiction.*

2

- *We believe in the concepts of full partnership, trust, and mutual assistance among the fire management agencies.*
- *We strongly support professionalism in all facets of fire management.*
- *We strive to bring the best talent to bear on vital issues in a timely manner, irrespective of agency affiliation.*
- *We strive for economy, efficiency, and quality in all activities, and practice concepts of total mobility, closest forces, and shared resources without geographic limitations.*
- *We constantly search for areas of agreement to further the effectiveness of the wildfire management program.*

Given our model of interagency and closest forces concept, we have agreed to accept each other's workforce qualifications and standards.

Federal requirements dictate that department and agency heads conduct a background investigation, adjudicate the results, and issue identity credentials to their employees and contractors who require long-term access to federally controlled facilities and/or information systems. It is not feasible for our fire agencies to put in place a system to conduct background checks of state and local employees and support the necessary credentials management program associated with those checks. We have identified approximately 90 separate wildland fire positions requiring some kind of logical access, comprising over 16,000 non-federal employees with the potential to receive a federal fire assignment, which could deploy them to any place in the United States on short notice. Implementing background check management programs would require that each of those thousands of employees be "sponsored" by a local unit of one of our agencies, that a background check be funded and adjudicated, the results of the adjudication be recorded, and the appropriate credentials be issued and managed.

Our analyses show that full compliance with background check requirements would cost approximately $3 million in annual direct costs, with significant additional costs for agency personnel to administer and manage the non-federal employee background check program. We have identified various alternatives for less than full background checks or for checking the backgrounds of sub-sets of non-federal employees. Those alternatives range from $500,000 to $1.5 million annually in direct costs – assuming that the alternatives could be implemented (with the approval of the General Services Administration, the Office of Personnel Management, and the Federal Bureau of Investigation would be required). These costs do not include the additional costs for agency personnel to administer and manage the non-federal employee program.

We believe there is minimal risk associated with granting these employees logical access when their duties so require. Each of these employees has been hired by a state or local entity and subject to appropriate vetting. In addition, these employees are "known" to the wildland fire community by virtue of holding a "red card" qualifying them for their fire duties.

Significant program risks are associated with either full implementation of the federal background check provisions, or preventing non-federal employees to gain logical access. In the first case, full implementation would require re-allocation of significant funds from direct response capability (firefighter salaries, necessary equipment, and so on) to pay for thousands of

background checks and hire a large staff to process and manage the resulting credentials. In the second case, loss of the non-federal workforce would significantly reduce the ability of the interagency community to provide dispatch service and incident management functions, placing the fire suppression support activities at significant risk, or increasing the risk of loss of public and private assets due to fire damage. The reduced ability to respond to fires, either by diversion of funding to support access management programs or through loss of the non-federal workforce, would reduce the current initial attack success rate (around 97% of all fires are caught in the first burning period). This reduction in successful initial attack would lead to more large fires and in the long-run drive the annual cost of fire suppression higher than the money spent to provide security background checks on non-federal cooperators. The final result would be an increase of suppression costs for both agencies and greater risks to firefighter and public safety.

The issues associated with implementation of federal background check requirements are detailed in Table 1, below.

Table 1: Implementation Issues Impacting USDA/DOI Business and Operational Capabilities

Issue #	Topic	Description	Expected Impacts
1	Fingerprinting: Electronically via Live Scan	There are a limited number of Live Scan machines in the field. In many cases it would be cost prohibitive to pay individuals for their travel and/or time while completing this task and in many cases these devices would require significant travel to get to. Live Scan machines are set up to be transmitted under an office's Submitting Office Identifier (SOI) or Submitting Office Number (SON). The state and local individuals requiring fingerprinting will not belong to that office's SON/SOI. Once transmitted via Live Scan, SON/SOI personnel will be charged for transmission activities. Results could take up to 24 hours. If fingerprints are not classifiable, results of the name check could take up to two weeks or longer, depending on common name and/or issues. If SON/SOI personnel are required to adjudicate these personnel they will have to be provided a means for reimbursement which will have to be covered under DOI or USDA budgets.	• Compensation for travel and/or time is unfunded. • SON/SOI may not be staffed to handle additional the workload • Unfunded liability burden on SON/SOI for Live Scan submissions • Extended adjudication periods do not meet business requirements for individuals who are not processed in advance • SON/SOI may not have the authority to adjudicate results

Issue #	Topic	Description	Expected Impacts
2	Fingerprinting: Hard Copy	Could have hard copy prints taken anywhere, however, some places, such as the local police station, may charge a fee for them to role the prints. We would need to supply the cards ahead of time so the individual can take the cards with them to the appointment. Fingerprint cards will need to be sent to a servicing Human Resource Office (HRO) so that they can be submitted and processed. These state and local individuals do not belong to a federal servicing HRO. Results can take up to 2 weeks. If prints are not classifiable, results of the name check could take up to two weeks or longer, depending on common name and/or issues. Agency personnel would be required to adjudicate these results at an increased cost and time both of which are currently unfunded for these individuals.	• Unexpected cost incurred for fingerprints taken at a local police station • Will need to reimburse employees for time and expense for this activity • SON/SOI may not be staffed to handle additional workload • Extended adjudication period does not meet business requirements for individuals who are not processed in advance • SON/SOI may not have the authority to adjudicate results • SON/SOI activities for these individuals are currently above and beyond normal work activities and unfunded by either agency
3	Fingerprinting: Credentialing Center:	While credentialing centers are located all over the US, they currently cannot be used for fingerprinting only. Further, in order to use a credentialing center, an individual must be "initiated" and "sponsored" by a federal agency before they can have their fingerprints captured. The cost of sending fingerprints using a credentialing center is more than sending from a live scan facility. There is also a GSA fee associated with the cost of each fingerprinting activity. Results could take up to 48 hours. Adjudication issues as described in items 1 and 2 above would also be a problem for this option	• Currently not an option under existing GSA contract. • May need to reimburse employees for time and expense for this activity depending on location and distance from a credentialing center • SON/SOI may not be staffed to handle additional workload • SON/SOI may not have the authority to adjudicate results • SON/SOI activities for these individuals are currently above and beyond normal work activities and unfunded by either agency

Issue #	Topic	Description	Expected Impacts
4	Background investigation:	A federal Human Resource Office (HRO) will need to initiate a background investigation request via the Electronic Questionnaires for Investigations Processing (eQIP) system. The state or local individual would be required to work with the HRO to complete the necessary online forms to facilitate the background investigation. Since these individuals are not serviced by a federal HR office, they would need to find an office willing to assume the workload to initiate, review, submit, and adjudicate results of the background investigation. Currently, HROs do not have the staff or resources to take on the additional workload for this group of individuals. The average turnaround time on a typical NACI is about 45 days.	• HRO currently does not have the staff to handle additional workload • SON/SOI may not have the authority to adjudicate results • Will need to reimburse employees for time and expense for this activity • SON/SOI may not be staffed to handle additional workload • SON/SOI may not have the authority to adjudicate results • SON/SOI activities for these individuals are currently above and beyond normal work activities and unfunded by either agency
5	Adjudication:	If these state or local individuals are subject to a federal background investigation and an HRO is unable to adjudicate favorably, there is currently no process in place to deal with an unfavorable adjudication. This unfavorable adjudication may have an impact on the individual's existing job (outside of wildland fire support). If a federal agency has the authority to conduct background investigations on this group of individuals, we will need to also develop some appeals process for them as well. This only exists for federal employees. State and local unions would likely need to be engaged in these discussions if any union members were part of this state/local group. If we are able to favorably adjudicate a background investigation, fire agencies must be willing to accept reciprocity so the process is not slowed down. Accepting reciprocity has historically been an issue among agencies.	• SON/SOI may not have the authority to adjudicate results • SON/SOI may not be staffed to handle additional workload • Cross Agency reciprocity must be put in place between the different Agency HR Offices to accept successful background adjudications

Issue #	Topic	Description	Expected Impacts
6	Tracking:	Currently, the only way to look up results of a fingerprint check and/or background investigation is either calling the Office of Personnel Management – Federal Investigative Services (OPM-FIS) or online thru the Central Verification System (CVS) or the Personnel Investigations Processing System (PIPS). Access is limited to federal adjudicators only. Also, PIPS/CVS does not indicate favorable adjudication on fingerprint results, it just indicates if there were issues or not. If fingerprints had issues, you would need to find the agency who submitted the fingerprints to see if they adjudicated favorably. Not all favorable adjudications are entered in PIPS/CVS for background investigations. If the favorable adjudication was not entered for a background investigation, you would need to find the agency who conducted the investigation to see if they were able to favorably adjudicate. Once results were received from these individuals, they would need to be stored in an agency accessible system. There is no tracking mechanism at this time that could store this information and make it readily available to agency personnel.	• SON/SOI may not have the authority to adjudicate results. • SON/SOI may not be staffed to handle additional workload to look up results or track • Some system would have to be implemented or an OPM process changed in order to make adjudication information easily available to agency personnel to support this business need
7	Funding:	The cost for fingerprinting and/or background investigating this group of individuals is not currently included in Agency budgets. The DOI and USDA estimates that 16,000 firefighters and support personnel, from various firefighting agencies covering 75,000 fire fighting districts, would need to be accounted for when estimating additional costs. Further, if this process becomes a responsibility for a federal HRO to complete, funding would need to be considered to help the HRO with staffing and resources. Current resourcing at most HROs is not sufficient to successfully handle the increased workload. Funding for additional position(s) and resources would need to be considered, in addition to the cost of the fingerprints and background investigations.	• SON/SOI may not be staffed to handle additional workload • Unfunded liability burden on background investigating and fingerprinting individuals • Need for funding to hire more HRO staff to support this need if risk is not accepted

Risks/Issues:

Per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, risk is defined as the following:

"Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence."

The following table contains potential issues/risks associated with allowing short-term state and local employees access to DOI/USDA general support systems. Some or all of these issues/risks may be mitigated with compensating controls which will be discussed in a later section of this document.

Table 2: Risks Related to Short-Term Employee Access to DOI/USDA IT Resources

Risk #	Description	Likelihood	Impact of Occurrence
1	A short-term state or local employees may be able to successfully implement a Denial of Service (DoS) attack against any of the fire center facilities	Believed to be low as this activity has been risk accepted for the previous 5 years without an occurrence of this risk to date. Technical controls in place to mitigate DoS attacks.	• Firefighter safety may be negatively impacted due to lack of communications availability • Potential litigation and financial impact as a result of personnel safety • Potential negative public relations impact due to harmful events
2	A short-term state or local employees may be able to successfully implement a Denial of Service (DoS) attack against a DOI or USDA General Support System (GSS)	Believed to be low as this activity has been risk accepted for the previous 5 years without an occurrence of this risk to date. Technical controls in place to mitigate DoS attacks. Network monitoring used to detect malicious activity.	• Potential litigation and financial impact as a result of delay in providing services to customer organizations both internal and external • Potential negative public relations impact due to service impacts to customer organizations
3	A short-term state or local employees may be able to successfully implement a Denial of Service (DoS) attack against one or more DOI or USDA Major Applications (MA)	Believed to be Low as this activity has been risk accepted for the previous 5 years without an occurrence of this risk to date. Technical controls in place to mitigate DoS attacks.	• Potential litigation and financial impact as a result of delay in providing services to customer organizations both internal and external • Potential negative public relations impact due to service impacts to customer organizations

Risk #	Description	Likelihood	Impact of Occurrence
4	A short-term state or local employees may be able to successfully compromise and exfiltrate sensitive USDA or DOI data	Believed to be low as this activity has been risk accepted for the previous 5 years without an occurrence of this risk to date. Role-based access controls provide least privilege, minimizing exposure to sensitive data.	• Potential litigation and financial impact as a result of data exfiltration activities • Potential negative public relations impact due to loss of data
5	A short-term state or local employees may be able to intentionally or unintentionally alter or delete USDA or DOI data	Believed to be low as this activity has been risk accepted for the previous 5 years without an occurrence of this risk to date. Role-based access controls provide least privilege.	• Vital information for making strategic or tactical decisions corrupted or unavailable • May impact responsiveness • Potential negative public relations impact due to a reduction in operational capabilities

Existing Mitigating Controls:

The following mitigating controls are already in place and will reduce the risk involved with this risk acceptance decision.

1. All management, operational, and technical IT security controls are inherited from the hosting agencies' General Support Systems and Major Applications, and applied to all users of the systems.
2. A Rules of Behavior document is signed by each short-term state or local individual before they are provided an account for use on the network.
3. All short-term employees are required to have IT security awareness training, including training on records management and privacy requirements before they are provided an account for use on the network.
4. DOI and USDA will use the "Red Card" to provide the acceptable level of assurance and public trust of firefighters and support personnel. The National Wildfire Coordinating Group sets minimum training and physical fitness standards for wild land firefighters. Red Cards are issued by various firefighting agencies that are members of the National Wildfire Coordinating Group. In some circumstances, local and rural firefighting agencies may issue letters of certification which are accepted by DOI and USDA.
5. Each short-term employee is assigned an individual temporary account that is only accessible for the duration of their detail. Such accounts are configured to require password reset at initial login.
6. All short-term accounts shall be documented detailing the link between the individual who receives the temporary account and actual account details. This documentation trail includes the short-term employee's signature recognizing their acceptance of their temporary access account.
7. Each short-term account's activities are logged, and this activity is traceable to the short-term employee assigned to that account during their detail.

8. DOI and USDA personnel perform account reviews for all short-term accounts on a periodic basis (at least once per assigned detail)

9. All fire response organizations and networks have Continuity of Operations Plans (COOP) in place and these plans are successfully tested at least once a year.

10. USDA networks have already implemented continuous monitoring functionality to ensure real-time alerting to network threats including fire network segments. DOI networks will provide this same capability in the near future.

11. Access to file servers shall be limited using Access Control Lists (ACLs) to ensure personnel are only allowed access to the information necessary to successfully complete their role within the organization.

12. All systems connecting to networked resources through DOI and USDA networks inherit security controls from their Trusted Internet Connection (TIC) certified gateways. This TIC infrastructure includes packet inspection, web content filtering and other network security functionality for all inbound and outbound traffic through these gateways.

13. All systems connecting to networked resources through USDA's network inherit security controls from their sensor array infrastructure which provides packet inspection, additionally USDA uses NetForensics and Big Fix to scan for and identify all threats to the network. Each application hosted on the NESS GSS inherits controls from USDA NITC and NESS and listed as child applications under the NESS ATO. NESS additionally provides DB protection to scan for and mitigate any risks in the application database.

14. All agency corporate GSS systems provided for short-term personnel use are configured with FDCC or USGCB settings (depending on the operating system level). Any deviations from these secure configuration settings are documented via the Plan of Action & Milestone (POA&M) process for the Agency providing the workstation and weakness completion verification forms (WCVFs) are utilized to document and accept risk where security configurations cannot be effectively implemented.

15. All systems display a warning banner at system startup reminding short-term personnel that they have no expectation of privacy while utilizing DOI or USDA provided systems.

16. All MA systems or agency corporate GSS systems required for short-term personnel utilization have a full Authorized to Operate (ATO). Minor applications needed to support work activities have been successfully documented as part of an overarching GSS or MA and have implemented or inherited all necessary controls to successfully remediate system risks to GSS or MA.

17. The sensitive data collected by the I-Suite system for time tracking and financial activities is encrypted using FIPS validated AES 256 bit encryption. This system is audited annually by USDA OIG, USFS CIO Security and by the USFS/USDA CFO to ensure compliance. The FY11 audit results were released in December 2011. The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module (for non-national security systems, the cryptographic requirements are defined by FIPS 140-2, as amended)

18. I-Suite Database Files: I-Suite uses Microsoft Desktop Engine (MSDE) which creates a separate file for each database. All database files are encrypted using 2048 bit Advanced Encryption Standard (AES). Database backup files are encrypted using this same encryption standard.
19. I-Suite Passwords: All user passwords are hashed using Secure Hashing Algorithm (SHA)-256 AES compliant hashing. The system creates a new randomly generated password during initial set-up and system password recovery. This password is saved using 256 bit AES compliant string encryption.
20. Social Security and Tax Identification Numbers: All social security and tax identification numbers are encrypted using 256 bit AES compliant string encryption.
21. The I-Suite system is configured to provide role-based least privilege access for all users. Backups of the I-Suite database and incident file server information are taken on a regular basis and such sensitive information is encrypted for storage or physical relocation.
22. I-Suite User Access Roles: The list below identifies the modules or functions of a module that a user can be granted access, not a type of user. For example, only users who need to input Time will be granted the Time module. A user can have access to more than one module or function, depending on their role. I-Suite defines the following categories of user access:
    a. Resources - Access to the Resources module and common and plans resource data
    b. Time - Access to the Time module and common and time resource data
    c. IAP - Access to the IAP module.
    d. Cost - Access to the Cost module and common and cost resource data
    e. Demob - Access to the Demob module and common, demob, and some plans resource data
    f. Supply Clerk - Access to the Supply module limited to non -management functions (No access to Setup, Import, and Export). Limited to only manage supply items identified with a "Supply Catalog Access" of "Supply Only" or "all."
    g. Supply Supervisor - Access to the Supply module limited to only manage supply items identified with a "Supply Catalog Access" of "Supply Only" or "all."
    h. Communications - Access to the Supply module limited to only manage supply items identified with a "Supply Catalog Access" of "Communications Only" or "all."
    i. Data Admin - Access to the Data Admin module
    j. DB Admin - Access to the DB Admin module
    k. Injury/Illness - Access to the Injury and Illness module
23. All desktop/laptop systems implement AntiVirus (AV) software which is properly installed, running and configured to download and implement the latest signature files available from the vendor or distributed through the agency's national operations center.
24. All desktop/laptop systems are configured to download and install all operating system critical updates from the operating system vendor as soon as these updates

are made available from the vendor or distributed through the agency's national operations center.

25. All desktop/laptop systems are configured to implement password-protecting, locking screensavers after some period of system inactivity in accordance with DOI/USDA policy (or in accordance with Authorizing Official (AO) documented deviation from such policy)
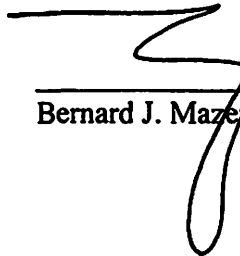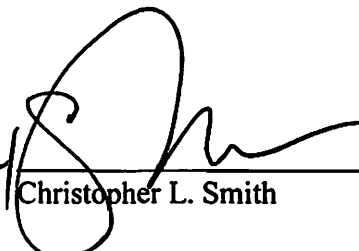
Residual Risks:

As shown in Table 2, there is residual risk associated with granting logical access to non-federal employees, even if full background check procedures are implemented. We believe that the set of existing twenty five mitigating controls described above can successfully remediate the residual risks to levels necessary for acceptance by Chief Information Officers.

Decision:

I approve this request.

(signature)   Z/16/24   _(signature)_   2/10/12
_____ _____
Bernard J. Mazer   Date   Christopher L. Smith   Date

I do not approve this request.

_____ _____
Bernard J. Mazer   Date   Christopher L. Smith   Date

I approve this request after the activities listed below have been successfully completed.

_____ _____
Bernard J. Mazer   Date   Christopher L. Smith   Date

I require the following additional information before I am willing to render a decision on this topic.

_____ _____
Bernard J. Mazer   Date   Christopher L. Smith   Date

**Information Technology Security Awareness Training Procedures
for Short-Term Non-Federal Emergency Response Personnel**

Background

The Department of the Interior (DOI) and the United States Department of Agriculture (USDA) employees are required to read and acknowledge their understanding of their respective Department's information Technology (IT) security awareness and individual user responsibilities prior to accessing IT systems or sensitive information.

Non-Federal employees (e.g., State and county fire team workers), specifically those that are assigned on-site for two weeks or less during the fire season, need to be rapidly trained and provisioned for their assignments. After discussion and review, DOI and USDA acknowledged the need for a streamlined security awareness training process that would meet the rapid deployment need and comply with federal security training requirements for this group of employees.

The following minimum requirements needed to be met to be accepted by both Departments:

1. Training must be consistent between the two Departments;
2. Accomplishment of training must be trackable;
3. Evidence of training must be readily available for review in the event of an audit; and
4. Training must meet the minimum security awareness training requirements for access to Federal IT systems and other sensitive information.

As part of the DOI/USDA training pilot, rapid deployment of training was determined to best be accomplished by using a combination of DOI/USDA IT Security Awareness and Best Practices handout and managed via a user log (reference Short-Term Emergency Response Personnel User Log) that tracks individual user's acknowledgement to adhere to the identified IT security best practices.

Scope

The process defined in this document is applicable to all short-term, non-Federal emergency response personnel who use DOI or USDA computer systems or have access to sensitive information, regardless of its form.

Oversight Responsibility

The benefiting Activity manager or Office Coordinator is responsible for ensuring that all short-term non-Federal emergency response personnel under their purview follow these procedures. The Activity manager or Office Coordinator may designate IT support personnel to distribute user accounts and coordinate with the Help Desk to reset accounts when they are no longer needed. The Activity manager or Office Coordinator shall make the user log available upon request for designated IT support personnel to review as needed. IT support personnel shall distribute user IDs and initial logon passwords in a sealed envelope.

If the non-Federal employee is deployed at multiple sites, the employee will be required to accomplish this training and acknowledge receipt of training at each site. The Aactivity Mmanagers or Office Coordinators at each site are required to log and track the training information as noted above.

Process

1. Short-term, non-Federal emergency response personnel shall be provided a copy of the *Information Technology Security Awareness and Best Practices* handout **before** they are granted initial access to their account.
2. The user shall read the *Information Technology Security Awareness and Best Practices* handout and contact their incident supervisor or the IT Security Manager if they have any questions. This is important in order to ensure that the user is aware of their responsibilities and to provide DepartmentDOI/office accountability.
3. The user shall fills out the *Short-Term Emergency Response Personnel User Log* and signs it to acknowledge their agreement to follow Department DOI IT security best practices. The Activity Mmanager or Office Coordinator shall initials the log signifying that the individual signed this acknowledgement.
4. The user shall receives a the sealed envelope with their account access information.

Short-Term Emergency Response Personnel User Log
Statement of IT Security Awareness and Individual User Responsibility for Government Computer Systems

I, the undersigned, upon reading the *Information Technology (IT) Security Awareness and Best Practices* document, agree to adhere to the identified IT Security Best Practices. I understand that when I use the DOI and/or USDA computer systems to gain access to any information therein, such use or access shall be limited to official Government business. Furthermore, I understand that any use of the aforementioned systems or information that is not official Government business may result in disciplinary action consistent with the nature and scope of such activity. All users of the DOI and/or USDA computer systems shall read and consent to the *Notice of Monitoring* prior to session initiation/logon.

Printed Name	Assigned Login	Detail Start Date	Detail End Date	Signature	Date	Coordinator On Duty

Information Technology Security Awareness Training
For Non-Federal, Short-Term Emergency Response Personnel

Select your servicing Department:	Select your incident assigned Agency/Bureau Emergency Response Center:
☐ US Department of Agriculture	☐ Bureau of Indian Affairs (BIA)
	☐ Bureau of Land Management (BLM)
	☐ Fish and Wildlife Service (FWS)
	☐ Forest Service (FS)
☐ US Department of the Interior	☐ National Park Service (NPS)
	☐ Office of the Secretary (OS)

Multiple laws and policies require that the Department of the Interior (DOI) have an effective and rigorous Information Technology (IT) security awareness program. Security is not just about technology, effective information security requires proper management and oversight. Computer and information security programs cannot be successful without management support and employee cooperation.

The difference between a secure computer system and one that is vulnerable is significantly affected by the manner in which employees adhere to security policies and measures. Security awareness is every employee's responsibility and is integral to the protection of DOI's IT and data assets. With decentralization of computer use and management, and increased use of mobile devices, there is increased potential for unauthorized access, modification, disclosure, and destruction of sensitive data.

Although outsiders (i.e., hackers, vandals, etc.) pose a threat to Government computers, a significant number of threats come from within DOI. Although most internal security breaches are unintentional in nature, some are targeted malicious attacks, or in many cases breaches occur due to a lack of education or awareness on the part of employees.

Computer User Responsibilities

As an authorized user of Federal information systems, you have certain responsibilities when using a Government computer. Any activity conducted on a Government system can be monitored. Each time you log on to a Government system, you consent to being monitored. You should use your computer for Government business only. In general, users must:

- Protect computer equipment and sensitive information you are authorized to access, including Privacy Act data and Personally Identifiable Information (PII).
- Perform your work activities using your individually assigned user identification (ID) and password.
- Ensure you are appropriately trained on the computer system(s) you access.
- Avoid Government computer misuse. Examples of computer misuse include viewing or downloading pornography, gambling on the Internet, conducting private commercial

- business activities or profit-making ventures, loading personal software, or making unauthorized configuration changes.
- If issued a mobile device (i.e., laptop, BlackBerry, iPad), keep it secure at all times and out of sight or in a completely secure location when not in use.
- Users should do their best to protect computer equipment from damage, abuse, theft, and unauthorized use.
- Keep unauthorized individuals away from your computer equipment and data.
- Do not throw away or recycle paper documents containing sensitive data - shred them! Destroy diskettes, CD/DVD-ROMs and other removable media before disposal. Consult your incident supervisor for proper disposal procedures.
- Part of physical security includes controlling the inventory of equipment that stores Federal information. When Government laptops are lost or stolen, so is the information that is stored on them. When you receive Government property, you are responsible for that equipment and for taking the necessary precautions to ensure that it is not lost or stolen. If that property is lost or stolen, immediately notify your incident supervisor and follow DOI procedures for reporting the loss. In addition to reporting the loss of the equipment, you must report the loss of the information that was on the equipment, and the significance of that lost information.

By using Government office equipment and information systems, employees must understand and consent to the following:

- Employees have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the Government may, for any lawful Government purpose, monitor, intercept, search, and seize any communication or data transiting or stored on this information system.
- Any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.
- Employee consent is final and irrevocable. Employees may not rely on any statements or informal policies purporting to provide them with any expectation of privacy regarding communications on Government systems, whether oral or written, by their incident supervisor or any other official, except by the DOI Chief Information Officer (CIO).

IT Security Incidents

Employees are required to report all IT security incidents to their incident supervisor. Some examples of IT security incidents are:

- Accessing a computer and gaining control for unauthorized activities.
- Viewing inappropriate web sites.
- Sending offensive email messages.
- Planting malicious code such as computer viruses.

Unauthorized access or misuse of Government computer systems may subject violators to criminal or civil penalties, or other adverse action. Unauthorized or illegal use may subject violators to prosecution.

2

Immediately report any suspected security incidents, privacy incidents, security vulnerabilities, loss of equipment or violations to your incident supervisor as soon as possible.

User ID and Passwords

Employees receive an individual user identification (ID) and password that is only to be used by the designated employee. The user may be prompted to change the password when logging in for the first time. User IDs and passwords are not to be disclosed or shared with anyone, including IT systems support personnel. If you believe your assigned user ID and password have been compromised, immediately notify your incident supervisor. **You are responsible for all activity logged under your user ID.**

Passwords are an important defense against intruders. Users must select strong passwords and protect them carefully. The following list contains DOI's password policy. All users using DOI computer systems **MUST** use strong passwords. Strong passwords have the following characteristics:

Password Policies

- Passwords will be twelve or more characters in length.
- Passwords are required to have at least one upper case and one lower case letter.
- Passwords will contain at least one numeric character (0, 1, 2, 3...9).
- Passwords will contain at least one special character (i.e., %, &, #, *, etc.).
- Passwords are to be changed at required intervals or, at a minimum, every 60 days.
- When changing your password, at least two characters shall be unique from the previous password. For example, do not reuse the same password or add a 1, 2, 3, etc., on the end or beginning (i.e. Secret#01, Secret#02, …).
- Passwords used to access Internet or remote systems shall be different from passwords used to access internal systems and applications.

Passwords will be changed at required intervals or any time you feel the possibility exists that it may have been compromised. Here are some basic guidelines to follow when creating passwords:

- **Do not** use personal information (i.e., telephone numbers, names of family members, pets, etc.) or dictionary words in any language for your passwords.
- **Do not** tape user IDs and passwords to desks, laptops, walls, or terminals, or write them down and store them in list finders, desk drawers, etc.
- **Do not** store user IDs and passwords in an unsecured computer file. This is especially important for laptop, notebook, and handheld computers since they are easy targets for theft.
- **Do not** use sequences or repeated characters. "12345678," "222222," "abcdefg," or adjacent letters on your keyboard do not help make secure passwords.

Violation of the password policy can result in cancellation of an account and potentially loss of future access.

Computer Log Off

Either log off or use a password protected screen saver when you are temporarily away from your workstation. Password protected screen savers shall comply with the password rules listed above. Users are responsible for all activity logged under their user ID, and can be held accountable for any violations that are traced to their account. As a best practice, log off your computer at the end of the workday.

Computer Viruses

At a minimum, computer viruses can be an annoyance; at their worst, they can destroy or steal the data on your computer's hard drive or network servers. Although anti-virus software is in use, your best defense is vigilance in the form of common sense. Never use software or other executable files obtained from the Internet; they may contain hidden viruses. Scan any media (i.e., CDs, DVDs, thumb drives, etc.) received from an outside source prior to accessing the information using any Federal computer.

The most common method of distributing computer viruses today is through email and the Internet. Beware of anything you do not recognize or are not expecting. Typical messages are worded as:

"For your information..."
"Here is that address you requested..."
"You've got to see this..."

The best way to handle this and any similar message is to delete it. **NEVER OPEN THE ATTACHMENT!**

Employees should keep in mind these simple rules:

- If the sender is someone you know, but the message and/or attachment is unexpected or suspicious, call the person to verify they sent it.
- Do not be tempted by jokes, e-cards, etc., from any source. Even if you know the sender, you really do not need to see the latest animated cartoon -- not at the risk of losing valuable data, impacting technical support personnel, and causing potential embarrassment to yourself or your department.
- Do not forward suspicious email messages to other users, including outside email addresses. If the email attachment does contain a virus, sending it on to others will probably succeed in further spreading the virus.
- If you believe your computer has been infected with a virus, please contact your incident supervisor for assistance.

Some Internet sites may also contain viruses and just visiting these sites can infect your computer. These viruses are commonly distributed through what is known as malicious code -- a small computer program that is downloaded and executed on your computer. Malicious code can be downloaded by clicking on a link or even running your mouse pointer across an object on the web page.

The best way to avoid viruses on malicious web pages is to avoid visiting unnecessary web sites. Limiting your browsing to web sites for conducting official business will significantly reduce this risk. (See the Internet Acceptable Use guidance below for more information).

By following these simple rules, you can help limit the spread of viruses and other malicious code.

Authorized Software

Only approved and authorized licensed software may be installed on Federal computers, and only by IT systems support personnel. Unauthorized software may conflict with or damage other software or its data, may contain malicious code, or be in violation of copyright laws. It is illegal to make unauthorized copies of copyrighted software.

Peer-to-Peer Access

Peer-to-peer (P2P) connections are a common avenue for the spread of computer viruses and spyware. The installation and use of unauthorized P2P applications can also result in significant vulnerabilities to DOI's networks, including exposure to unauthorized access of information and compromise of network configurations.

Users are prohibited from using (P2P) file sharing. P2P file sharing poses a threat to IT security. It allows employees to transfer files between computers without proper security controls. These programs can be used to distribute inappropriate materials, violate copyright law, and put Government information at risk.

Physical Security

Physical security includes protection of the entire facility, from the outside perimeter to offices inside the building, including all of the information systems and infrastructure.

Employees should:

- Be aware of their surroundings at all times – ensure only authorized individuals are allowed in areas with restricted access.
- Make sure doors remain locked and secured (do not leave doors propped open).
- Report suspicious activity to your incident supervisor.
- Secure your equipment, records, and data when you leave the office each day.
- Keep official items such as a badges, keys, laptops, mobile phones, documents, CDs, etc. completely secure at all times, and ensure unauthorized personnel do not gain access to them

as they may be used to gain access to restricted information or DOI areas. Report the loss or theft of such items to your incident supervisor immediately.

Social Engineering

Social engineering is a hacking technique that relies on human nature. This approach is used by many hackers to obtain information valuable to accessing a secure system.   Rather than using software to identify security weaknesses, hackers use social engineering to trick an individual into revealing passwords and other information that can be used to compromise your system security. Hackers use people's inherent nature to trust other people to learn passwords, logon IDs, server names, operating systems, or other sensitive information.

Understanding social engineering behaviors will enable you to recognize and avoid providing important security information to unauthorized sources. For example, a hacker may attempt to gain system information from an employee by posing as a service technician or system administrator with an urgent access problem.

Nobody should ever ask you for your passwords. This includes system administrators and help desk personnel. If someone says they need your password, they are lying, do not give it to them. If you suspect someone is using social engineering to gain access to DOI information, contact your incident supervisor immediately.

Improper Use of Government Office Equipment

Unauthorized or improper use of Government office equipment may result in disciplinary action, as well as civil and criminal penalties. The following rules apply when using Government office equipment, including computers, printers, telephones, fax machines, etc.:

Employees are prohibited from using Government office equipment, Internet access, and e-mail for personal uses except as authorized by DOI policy.

- Employees are prohibited from using Government office equipment for activities that are illegal (e.g., gambling) or that are inappropriate or offensive to co-workers or the public, such as sexually explicit material or remarks that ridicule others on the basis of race, creed, religion, color, sex, disability, age, national origin, or sexual orientation.
- Employees are prohibited from using Government office equipment at any time for any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in political activities.
- Employees are prohibited from using Government office equipment at any time to make purchases for personal commercial gain activity.
- Employees are not authorized to remove Government property from the office for personal use.
- Employees are prohibited from using Government-provided access to the Internet to present their personal views in a way that would lead the public to interpret it as an official Government position. This includes posting to external news groups, blogs, or other public forums.

- Employees are prohibited at any time from using the Internet as a radio or music player. Such live stream use of the Internet could impact network performance and significantly slow communications, inhibiting employees from conducting official business.
- Employees are prohibited at any time from using "push" technology on the Internet or other continuous data streams, unless they are directly associated with the employee's job. Push technology from the Internet means daily, hourly or continuous updates via the Internet (i.e., news, stock quotes, weather, and similar information). Continuous data streams could degrade the performance of the entire network.

Internet Acceptable Use
It is the policy of DOI to allow and encourage the use of Internet services to support the accomplishment of the various missions of DOI. Users of the Internet must be aware of the following policies regarding the content and management of Internet data and information.

- Federal Government telecommunication systems and equipment (including Government owned telephones, facsimile machines, electronic mail, interact systems (Internet)), and commercial systems (when used is paid for by the Federal Government) shall be for official use and authorized purposes.
- Authorized Internet use may include limited personal use, with incident supervisor approval, and it is determined that such use:

  o Does not adversely affect the performance of official duties by the employee or the employee's organization.
  o Is of reasonable duration and frequency, and whenever possible, made during the employee's personal time such as after duty hours or lunch periods.
  o Serves a legitimate public interest (such as educating the employee on the use of the technology, enhancing the professional skills of the employee, job searching in response to Federal Government downsizing).
  o Do not use Federal Government systems for activities that would reflect adversely on DOI or the Agency/Bureau, such as uses involving pornography, playing on-line games, conducting personal commercial activities, distributing chain letters, unofficial advertising, lobbying, or active political activity, violations of statute or regulation, or other uses that are incompatible with public service.
  o Does not overburden DOI telecommunications (as may be the case with large broadcasts and group mailings), and create no significant additional cost to DOI.
  o Does not compromise the security of any Government host computer.

Sensitive and Privacy Act Data

Sensitive information is defined as:

Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. [15 USC Sec. 278-g3].

Examples of sensitive data include Privacy Act Data and PII pertaining to an individual (i.e., social security numbers, date of birth, credit card number, home addresses, etc.), pending contract-related information, certain financial records, and other information that if disclosed could be detrimental to an employee's privacy or DOI's mission. Sensitive data must not be stored on your computer's local hard drive unless it is encrypted. Sensitive data must only be stored on Government issued removable media (CD/DVD-ROM's, thumb drives, etc.); shall be encrypted requiring a strong password for decryption; and locked away in a secure location when not in use. Non-Government furnished equipment or storage media shall not be connected to DOI's network or used to transmit information in any way.

When disposing of removable media containing sensitive data, the data must be overwritten using authorized tools or the media must be physically destroyed before discarding. **<u>Simply erasing files is not enough</u>** because erased files can be easily retrieved. Consult your incident supervisor for proper disposal procedures for removable media.

Sensitive data will only be transmitted to or stored on DOI controlled equipment or incident supervisor approved locations. Sensitive data shall be encrypted when transmitting to authorized locations. Consult your incident supervisor if you have any questions about what is an authorized or unauthorized location, or how to protect sensitive data.

Employees must understand the following responsibilities to maintain the confidentiality of Privacy Act data and to protect sensitive data:

- Use privacy sensitive information only for the purpose it was collected.
- Disclose sensitive or privacy information only to authorized personnel on a "need to know" basis.
- Limit access to sensitive/privacy information.
- Do not send any sensitive/privacy information to any internet site or personal email address. Doing so violates DOI policy as information transferred outside of DOI's network may not be encrypted or secure. Contact your incident supervisor for approval prior to transmitting sensitive/privacy information to a non-Government furnished system or account.
- Contact your respective Agency/Bureau Privacy Officer if you have any questions regarding the management of privacy sensitive information.

- If you receive an e-mail that contains privacy information that does not belong to you in the subject, body or attachment(s) of the message, **<u>DO NOT</u>** forward it to anyone. Contact your incident supervisor for further guidance.
- **<u>Immediately</u>** report any suspected loss or compromise of privacy information to your incident supervisor. *DOI must report suspected privacy information breaches to U.S. CERT <u>within **1 hour** of discovery.</u>*

Records Management

DOI has a legal requirement to protect the information it collects and maintains on employees and the public, to preserve and manage the Federal records in its custody, and promote transparency in our Government operations.   It takes both management support and employee cooperation for DOI to successfully meet its information management obligations.   Failure to follow these requirements may lead to disciplinary action up to and potentially including removal, and could also be the basis for lawsuits and civil or criminal penalties; therefore it is of the utmost importance that all employees understand their information management responsibilities.

- Recognize the importance of DOI records.   A record is any item, in any physical form (paper, email, electronic file, CD, voice clip, video clip, social media, etc.) that advances or represents DOI work. All information in any form (email, paper, electronic files, photographs, etc.) that record DOI functions, decisions, and actions taken as part of your work at DOI should be saved.
- DOI records are the property of the Federal Government, not the property of individual employees, and cannot be used except as explicitly authorized in writing by DOI and must not be removed from the custody and control of DOI upon the employee's departure.
- Ensure the appropriate levels of safeguards are implemented to protect records in your possession, especially records that contain sensitive information and do not destroy or alter existing records without explicit authorization from your incident supervisor.
- Preserve all records associated with a preservation or litigation hold. Your incident supervisor will identify any categories of such records and provide additional guidance.
- Do not release any DOI records. Refer all requests for information or records to your incident supervisor for follow up action with their respective Agency/Bureau Freedom of Information Act (FOIA) Officer.

Service Level Agreement

Between: _____ **and**
_____
Dispatch Center Name   Department Servicing IT
Organization

I. PURPOSE

This service level agreement establishes guidelines to be employed in support of the _____ in its role of providing district coordination and dispatching support via networked computers which are utilized by a variety of temporarily detailed, short-term, non-federal emergency response personnel. Specifically, it defines security procedures and processes to initiate and maintain user profiles and passwords for the Dispatch Center computers on the Servicing Agency Information Technology (IT) corporate network.

II. RESPONSIBILITIES

The Servicing Agency (IT) Specialist in their role of system administrator will establish, maintain, and reset necessary user profiles (also referred to as user IDs) for short-term non-federal emergency response personnel. The user ID and password will be provided to the Dispatch Center Manager or Office Coordinator in a sealed envelope that has been signed across the seal. The Dispatch Center Manager or Office Coordinator will keep these user IDs in a secure location and manage their distribution to all short-term, non-federal emergency response personnel while ensuring accountability of the secure user IDs and passwords. The Dispatch Center Manager or Office Coordinator will notify the Servicing Agency IT Specialist when short-term, non-federal emergency response personnel terminate and the user ID password is reset and the ID is available for reuse.

III. OPERATIONAL PROCEDURES

The Servicing Agency IT Specialist will initially create _____ [1] user accounts and provide a list of them along with the sealed envelopes containing account IDs and passwords to the Dispatch Center Manager or Office Coordinator. The Dispatch Center Manager or Office Coordinator will keep these items in a secured area. When short-term, non-federal emergency response personnel are requested and report to work, the Dispatch Center Manager or Office Coordinator will distribute the information packet that contains the IT Security Awareness and Best Practices handout. The user will read the IT Security Awareness handout, fill out the *Short-Term Emergency Response Personnel User Log* and sign it to acknowledge agreement to follow Servicing Agency IT Security best

---

[1] Recommend number of workstations x 3 to accommodate possible off hour provisioning needs.

practices.   The user receives a sealed envelope that contains the user's assigned ID and password. During initial login, the user will be prompted to immediately change the provided password to a strong password, which will only be used by that user. Any required password reset or account unlock activity will need to be coordinated with the user's dispatch supervisor. When the user's assignment is completed, the Dispatch Center Manager or Office Coordinator is notified and the user ID profile list is documented with the date released. The Dispatch Center Manager or Office Coordinator notifies the Servicing Agency IT Specialist that the user ID is available for reuse and a new password is requested.

Dispatch Center Manager or Office Coordinator	Date	Fire Management Officer	Date

Information Technology Manager or Specialist	Date