



WASHINGTON



THE DEPARTMENT OF AGRICULTURE

FEB 17 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

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 defined 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.*

- *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.	<ul style="list-style-type: none"> • 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	<p>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.</p>	<ul style="list-style-type: none"> • 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:	<p>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</p>	<ul style="list-style-type: none"> • 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:	<p>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.</p>	<ul style="list-style-type: none"> • 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:	<p>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.</p>	<ul style="list-style-type: none"> • 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:	<p>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.</p>	<ul style="list-style-type: none"> • 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:	<p>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.</p>	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.

