ORDER FOR SUPPLIES OR SERVICES

1. CONTRACT/PURCH ORDER/AGREEMENT NO.	2. DELIVERY ORDER/CALL NO.	3. DATE OF ORDER/CALL (YYYYMMMDD)	4. REQUISITION/PURCH REQUEST NO.	5 PRIORITY
DTOS59-09-D-00467	DTMA-91-F-2011-000028/0002	11/29/2011	MA-PR614-20120019	

6. ISSUED BY CODE 00091

U.S. DOT/ Maritime Administration
Office of Acquisition MAR-380
1200 NEW JERSEY AVENUE SE
MAIL STOP W-28-201
WASHINGTON DC 20590-0001

7. ADMINISTERED BY (If other than 6) CODE 00091

U.S. DOT/Maritime Administration
Office of Acquisition
MAR-380
1200 New Jersey Avenue, SE
Mail Stop W-28-201
Washington DC 20590-0001

8. DELIVERY FOB
- [X] DESTINATION
- [ ] OTHER (See Schedule if other)

9. CONTRACTOR CODE 541878254 FACILITY

NAME AND ADDRESS
ActioNet Inc
Attn: Adrienne Kipps-Spanagel
2600 Park Tower Drive
Suite 1000
Vienna VA 22180-7370

10. DELIVER TO FOB POINT BY (Date) (YYYYMMMDD)
Multiple

11. X IF BUSINESS IS
- [ ] SMALL
- [X] SMALL DISADVANTAGED
- [X] WOMEN-OWNED

12. DISCOUNT TERMS

13. MAIL INVOICES TO THE ADDRESS IN BLOCK
PO Box 25710 OK

14. SHIP TO CODE

Multiple Destinations

15. PAYMENT WILL BE MADE BY CODE

MARAD A/P INVOICES
P.O.BOX 25710
OKLAHOMA CITY OK 73125

MARK ALL PACKAGES AND PAPERS WITH IDENTIFICATION NUMBERS IN BLOCK 1 AND 2.

16. TYPE OF ORDER
- DELIVERY/CALL [X] This delivery order/call is issued on another Government agency or in accordance with and subject to terms and conditions of above numbered contract.
- PURCHASE [ ] Reference your _____ furnish the following on terms specified herein.

ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.

NAME OF CONTRACTOR	SIGNATURE	TYPED NAME AND TITLE	DATE SIGNED (YYYYMMMDD)
ActioNet, Inc.		Adrienne Kipps-Spanagel, Contract Administrator	11/30/2011

[X] If this box is marked, supplier must sign Acceptance and return the following number of copies: 1

17. ACCOUNTING AND APPROPRIATION DATA/LOCAL USE

70XR161710.2012.93040ADP00.1261000000.25704.61006600 / 7012613040ADP0

18. ITEM NO.	19. SCHEDULE OF SUPPLIES/SERVICES	20. QUANTITY ORDERED/ ACCEPTED*	21. UNIT	22. UNIT PRICE	23. AMOUNT
	LIST OF CHANGES: Continued ...				

*If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity ordered and encircle.

24. UNITED STATES OF AMERICA
BY: Benedict J. Burnowski CONTRACTING/ORDERING OFFICER

25. TOTAL $214,240.00

26. DIFFERENCES

27a. QUANTITY IN COLUMN 20 HAS BEEN
- [ ] INSPECTED
- [ ] RECEIVED
- [ ] ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED:

b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

c. DATE (YYYYMMMDD)

d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE

f. TELEPHONE NUMBER

g. E-MAIL ADDRESS

28. SHIP. NO.

29. D.O. VOUCHER NO.

30. INITIALS

31. PAYMENT
- [ ] PARTIAL
- [ ] FINAL

32. PAID BY

33. AMOUNT VERIFIED CORRECT FOR

34. CHECK NUMBER

35. BILL OF LADING NO.

36. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT.

a. DATE (YYYYMMMDD)

b. SIGNATURE AND TITLE OF CERTIFYING OFFICER

- [ ] COMPLETE
- [ ] PARTIAL
- [ ] FINAL

37. RECEIVED AT	38. RECEIVED BY (Print)	39. DATE RECEIVED (YYYYMMMDD)	40. TOTAL CONTAINERS	41. S/R ACCOUNT NUMBER	42. S/R VOUCHER NO.

NAME OF OFFEROR OR CONTRACTOR
ActioNet Inc

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
	Reason for Modification : Funding Only Action Total Amount for this Modification: $0.00 New Total Amount for this Version: $0.00 New Total Amount for this Award: $559,710.00 Period of Performance: 07/01/2011 to 06/30/2016				
0007	Contract DTMA-91-F-2011-00028: Fund LOA applied to CLIN 0001 - Direct Labor - 2,200 Manhours - ($194,500) Delivery: 06/30/2012 Delivery Location Code: MAR-614-1 Channing Jones 1200 New Jersey Avenue, SE Washington DC 20590 USA Amount: $194,500.00				194,500.00
0008	Contract DTMA-91-F-2011-00028: Fund LOA applied CLIN 0002 - Travel/ODCs ($19,740) Delivery: 06/30/2012 Delivery Location Code: MAR-614-1 Channing Jones 1200 New Jersey Avenue, SE Washington DC 20590 USA Amount: $19,740.00				19,740.00
0009	Acquisition Policy Memo(APL)-2011-02- Contractors Personnel Security and Agency Access clause provisions are instituted and made a part of this task order in accordance with interim clause requirements for guidance where contractor staff require physical access to federally controlled or logical access to Federal/ Department Information systems. Policy is to provide guidance for the following area: Risk and Sensitivity Level Designations, Pre-screening of Contractor Employees, Citizenship and Alien Status, Background Investigation and Adjudication, Agency Access Denied, Identification Card Application Process, Identification Card Custody and Control, Surrender of ID Cards, and Use of this Clause. Delivery: 06/30/2016 Delivery Location Code: 00091 U.S. DOT/Maritime Administration Office of Acquisition MAR-380 1200 New Jersey Avenue, SE MAIL STOP W-28-201 Continued ...				0.00

NAME OF OFFEROR OR CONTRACTOR
ActioNet Inc

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
	Washington DC 20590-0001 USA Amount: $0.00 Accounting Info: - $0.00 (Subject to Availability of Funds) Ready Reserve Force Management System (RMS) IT Operations and Management support services. This task order funding provided by the following purchase request: MA-PR614-20120019 items#0001-0002 is $214,240.00. The following clause provisions are instituted and made a part of this task order in accordance with interim clause requirements, ¿Acquisition Policy Memo(APL)-2011-02- Contractors Personnel Security and Agency Access¿, for guidance where contractor staff require physical access to federally controlled or logical access to Federal/ Department Information systems. Line of accounting 70XR161710.2012.9340ADP00.1261000000.25704.61006600/7012613040ADP0 in the amount for CLIN 0001 $194,500 and CLIN 0002 $19,740 for a total obligated amount of $214,240.00. The beginning balance of the modification was $559,710.00 with the addition of $214,240.00 the new ending balance is $773,950.00				

Department of Transportation
Office of the Senior Procurement Executive

No. APL-2011-02
Date 11/09/2011

DOT ACQUISITION POLICY LETTER

This Acquisition Policy Letter is issued under the authority of the Senior Procurement Executive of the Department of Transportation

Subject: **Contractors Personnel Security and Agency Access**

References:

- Homeland Security Presidential Directive – 12 (HSPD -12)
- Federal Information Processing Standards Publication (FIPS PUB) Number 201.
- Federal Acquisition Regulation Clause - 52.204-9 "Personal Identity Verification of Contractor Personnel.

When is this Acquisition Policy Letter (APL) Effective?

This APL is effective November 9, 2011.

When Does This APL Expire?

This APL remains in effect until the resulting policy is incorporated into the Transportation Acquisition Regulation (TAR) or otherwise cancelled.

Who is the Point of Contact?

Contact Jeffrey Thomas of the Office of the Senior Procurement Executive, (202) 366-4226 or by email at Jeff.Thomas@dot.gov. For technical questions regarding the implementation of the clause requirements, contact Linda Guier of the Office of Security at (202) 366-6514.

Visit our website at http://www.dot.gov/ost/m60/ for additional information on DOT Acquisition Policy Letters and other policy issues.

What is the Purpose of this APL?

This APL supports deployment of HSPD-12 and FIPS PUB 201 through the issuance of contract language for use in all solicitations and contracts where contractor staff require routine access to federally controlled facilities and/or require logical access to Federal or Departmental information systems. This

APL supersedes the memo entitled "Contract Requirements – Homeland Security Presidential Directive 12 (HSPD- 12)," dated June 22, 2010. This APL applies to all DOT operating administrations, except for the Federal Aviation Administration.

What is the Background?

On August 27, 2004, President Bush issued Homeland Security Presidential Directive 12 (HSPD-12), entitled "Policy for a Common Identification Standard for Federal Employees and Contractors." This directive required the development and implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors. As required by the directive, the Department of Commerce issued Federal information processing Standard Publication Number 201 (FIPS PUB 201), Personal Identity Verification of Federal Employees and Contractors. FIPS PUB 201 provides detailed specification for identification issued by Federal departments and agencies to Federal employees and contractors for gaining physical access to Federally controlled facilities and logical access to Federal information systems. In support of these requirements the Federal Acquistion Regulation issued clause 52.204-9 "Personal Identity Verification of Contractor Personnel" which required contractors to comply with PIV process for all affected employees in accordance with agency procedures identified in the contract. This new DOT clause describes those agency procedures.

What is the Guidance?

1. Contracting officers shall insert the interim clause provided in Attachment (1) "DOT Contractor Personnel Security and Agency Access" (October 2011) into all solicitations and contracts (including Task Orders, if appropriate) where contractor staff require physical access to federally controlled facilities or logical access to Federal/Departmental information systems.

2. No later than December 31, 2011, contracting officers shall modify existing contracts (or task orders) to include "DOT Contractor Personnel Security and Agency Access" (October 2011), where contractor staff require physical access to federally controlled facilities or logical access to Federal/Departmental information systems.

3. Attachment 2 provides contracting officers and contracting officers technical representatives additional guidance on determining the Contract Risk Designation and Sensitivity levels.

Jeffrey Thomas
Associate Director
Acquisition Policy & Oversight (M61)
Office of the Senior Procurement Executive

Attachment

Attachment 1

U.S DEPARTMENT OF TRANSPORTATION (DOT)

CONTRACTOR PERSONNEL SECURITY AND AGENCY ACCESS

(NOVEMBER 2011)

The following definitions are provided:

- "Agency Access" means access to DOT facilities, sensitive information, information systems or other DOT resources.
- "Applicant" is a contractor employee for whom the contractor submits an application for a DOT identification card.
- "Contractor Employee" means prime contractor and subcontractor employees who require agency access to perform work under a DOT contract.
- "Identification Card" (or "ID card") means a government issued or accepted identification card such as a Personal Identity Verification (PIV) card, a PIV-Interoperable (PIV-I) card from an authorized PIV-I issuer, or a non-PIV card issued by DOT, or a non-PIV card issued by another Federal agency and approved by DOT. PIV and PIV-I cards have physical and electronic attributes that other (non-PIV) ID cards do not have.
- "Issuing Office" means the DOT entity that issues identification cards to contractor employees.
- "Local Security Servicing Organization" means the DOT entity that provides security services to the DOT organization sponsoring the contract.

1. Risk and Sensitivity Level Designations – For contracts requiring access to DOT facilities, sensitive information, information systems or other DOT resources, the contractor employees will be required to complete background investigations, identity proofing, and government identification card application procedures to determine suitability for access. DOT will assign a risk and sensitivity level designation to the overall contract and/or to contractor employee positions by category, group or individual. The risk and sensitivity

level designations will be the basis for determining the level of personnel security processing required for contractor employees.

IF THE DESIGNATED RISK IS:	THE BACKGROUND INVESTIGATION IS:
Low	National Agency Check with Written Inquiries (NACI)
Moderate	Minimum Background Investigation (MBI)
High	Background Investigation (BI)

Contractor employees may also be required to obtain security clearances (i.e., Confidential, Secret, or Top Secret). National Security work designated "special sensitive," "critical sensitive," or "non-critical sensitive" will determine the level of clearance required for contractor employees. Personnel security clearances for national security contracts in DOT will be processed according to the Department of Defense National Industrial Security Program Operating Manual (NISPOM).

2. Pre-screening of Contractor Employees - The contractor must pre-screen individuals designated for employment under any DOT contract by verifying minimal suitability requirements to ensure that only quality candidates are considered for contract employment, and to mitigate the burden on the Government of conducting background investigations on objectionable applicants. The contractor must exercise due diligence in pre-screening all employees prior to submission to DOT for agency access. DOT may decline to grant agency access to a contractor employee for reasons including, but not limited to:
   a) Conviction of a felony, a crime of violence, or a misdemeanor involving moral turpitude.
   b) Falsification of information entered on forms or of other documents submitted.

c) Improper conduct including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct adverse to the Government regardless of whether the conduct is directly related to the contract.

d) Any behavior judged to pose a potential threat to DOT facilities, sensitive information, information systems or other resources.

3. Citizenship and Alien Status - The contractor must monitor an alien's continued authorization for employment in the United States. The contractor must provide documentation to the Contracting Officer or the Contracting Officer's Technical Representative during the background investigation process that validates that the E-Verify requirement has been met for each contractor employee.

4. Background Investigation and Adjudication – The contractor employee must have a favorable adjudication of background investigation before DOT will issue an ID card to the contractor employee granting access to DOT facilities, sensitive information, information systems or other DOT resources. DOT may accept favorable adjudications of background investigations from other Federal agencies when applicants have held PIV cards issued by those agencies with no break in service. DOT may also accept PIV-I (interoperable) cards issued by an authorized PIV-I issuer as evidence of identity. A favorable adjudication does not preclude DOT from initiating a new investigation when deemed necessary. At a minimum, the FBI National Criminal History Check (fingerprint check) must be favorably completed before a DOT identification card can be issued. Each contractor must use the Office of Personnel Management's (OPM) e-QIP system to complete any required investigative forms. Instructions for obtaining fingerprints will be provided by the COTR or CO. The DOT Office of Security, M-40, or a DOT organization delegated authority by M-40, is responsible for adjudicating the suitability of contractor employees.

5. Agency Access Denied – Upon contract award, DOT will initiate the agency access procedure for all contractor employees requiring access to DOT facilities, sensitive information,

information systems and other DOT resources for contract performance. DOT may deny agency access to any individual about whom an adverse suitability determination is made. Failure to submit the required security information or to truthfully answer all questions shall constitute grounds for denial of access. The contractor must not provide agency access to contractor employees until the COTR or CO provides notice of approval, which is authorized only by the DOT Office of Security (M-40) or a DOT organization delegated authority by M-40. Where a proposed contractor's employees are denied agency access by the Government or, if for any reason proposed applications are withdrawn by the contractor during the agency access process, the additional costs and administrative burden for conducting additional background investigations caused by a lack of effective pre-screening or planning on the part of the contractor may be considered as part of the contractor's overall performance evaluation.

6. Identification Card Application Process - The COTR will be the DOT ID card Sponsor and point of contact for the contractor's application for a DOT ID card. The COTR shall review and approve the DOT ID card application before an ID card is issued to the applicant.

   An applicant may be issued either a Personal Identity Verification (PIV) card that meets the standards of Homeland Presidential Security Directive (HSPD-12), or an applicant may be issued a non-PIV card. Generally, a non-PIV card will be issued for contracts that expire in six months or less, including option periods. The COTR may request the issuing office to waive the six month eligibility requirement when it is in DOT's interest for contract performance.

   The applicant must complete a DOT on-line application for a PIV card. For a non-PIV card, the applicant must complete and submit a hard copy of Form 1681 to the COTR/Sponsor. Regardless of the type of card to be issued (PIV or non-PIV), the applicant must appear in-person to provide two forms of identity source documents in original form to DOT. The identity source documents must come from the list of acceptable documents included in *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification*. At least one document

must be a valid State or Federal government-issued picture identification. For a PIV card, the applicant may be required to appear in-person a second time for enrollment and activation.

7. Identification Card Custody and Control – The contractor is responsible for the custody and control of all forms of government identification issued by DOT to contractor employees for access to DOT facilities, sensitive information, information systems and other DOT resources. The contractor must immediately notify the COTR or, if the COTR is unavailable, the CO when a contractor employee no longer requires agency access due to transfer, completion of a project, retirement, removal from work on the contract, or termination of employment.

The contractor is responsible for maintaining and safeguarding the DOT ID card upon issuance to the contractor employee. The contractor must ensure that contractor employees comply with DOT requirements concerning the renewal, loss, theft, or damage of an ID card. The contractor must immediately notify the COTR or, if the COTR is unavailable, the CO when an ID card is lost, stolen or damaged.

Failure to comply with the requirements for custody and control of DOT ID cards may result in withholding final payment or contract termination based on the potential for serious harm caused by inappropriate access to DOT facilities, sensitive information, information systems or other DOT resources.

a) Renewal: A contractor employee's DOT issued ID card is valid for a maximum of three years or until the contract expiration date (including option periods), whichever occurs first. The renewal process should begin six weeks before the PIV card expiration date. If a PIV card is not renewed before it expires, the contractor employee will be required to sign-in daily for facility access and may have limited access to information systems and other resources.

b) Lost/Stolen: Immediately upon detection, the contractor or contractor employee must report a lost or stolen DOT ID card to the COTR, or if the COTR is unavailable, the CO, the issuing office, or the local servicing security organization. The contractor must submit an incident report within 48 hours, through the COTR or, if the COTR is unavailable, the CO, the issuing office, or the local security servicing organization describing the circumstances of the loss or theft. The contractor must also report a lost or stolen PIV card through the DOT on-line registration system. If the loss or theft is reported by the contractor to the local police, a copy of the police report must be provided to the COTR or CO. From the date of notification to DOT, the contractor must wait three days before getting a replacement ID card. During the 3-day wait period, the contractor employee must sign in daily for facility access.

c) Replacement: An ID card will be replaced if it is damaged, contains incorrect data, or is lost or stolen for more than 3 days, provided there is a continuing need for agency access to perform work under the contract.

8. Surrender of ID Cards – Upon notification that routine access to DOT facilities, sensitive information, information systems or other DOT resources is no longer required, the contractor must surrender the DOT issued ID card to the COTR, or if the COTR is unavailable, the CO, the issuing office, or the local security servicing organization in accordance with agency procedures.

9. Use of This Clause - The contractor is required to include these clauses in any subcontracts that require the subcontractor or subcontractor's employees to have access to DOT facilities, sensitive information, information systems or other resources.

Attachment 2

BACKGROUND AND GUIDANCE FOR CO/COTR:

Contract Risk Designation and Sensitivity Levels Definitions -

Risk Designation – an assessment of a position (low, medium, high) to determine its potential adverse impact to the integrity or efficiency of the service, its effect on the agency or on the agency's mission.

Sensitivity Designation – Each position in the Federal service not designated Non-sensitive must be designated as Noncritical-sensitive, Critical-Sensitive, or Special-Sensitive, depending on the degree to which, by virtue of the nature of the position, the occupant could bring about a material adverse effect on the national security. The nature of the position includes the incumbent's foreseeable need for access to classified information; under E.O. 12968, eligibility for access to classified information cannot be granted unless such access is clearly consistent with the national security. The nature of the position also includes the level of clearance required (i.e., confidential, secret, top secret); under E.O. 12958, as amended, the level at which information is classified depends on whether unauthorized disclosure reasonably could be expected to cause "damage," "serious damage," or "exceptionally grave damage" to the national security.

The contract designation is determined by evaluating the risk or sensitivity of the work being planned; the risk or sensitivity of the facility upon or in which the work is to be performed; the security impact level of the IT system to which personnel have access; the level of access privileges to an IT system; whether the contracted activities are to be performed during or outside of normal work hours; and the extent that Government escort will be both necessary and available to the contract employees present in the facility or while IT access is required. The contract designation also determines the security/suitability requirements for the contract personnel who will perform the work. The costs for conducting the applicable security/suitability background checks are to be absorbed by the program office sponsoring the procurement or

included into the contract language for the contractor to absorb.

The risk or sensitivity level designation shall be made by the program office representative (typically the CO or COTR), in conjunction with the operating unit management, M-40, CIO's office, and the procurement office. The COTR will review the work to be performed under the contract and assign the highest risk designation to the entire contract in accordance with the criteria stated below. A risk-based, cost effective approach must be followed to determine the risk of harm to DOT systems, employees or facilities in comparison to the opportunity for personnel to cause harm. The rationale for the designated risk level shall be documented and placed in the official contract file. Accordingly, each contract employee will undergo investigative processing based on the contract risk level designation per Chapter 5 of the DOT Order 1630.2B Personnel Security Manual. The contractor shall not provide access to employees until M-40, or a DOT organization delegated authority by M-40, provides official notice to the COTR.

High Risk – A contract shall be designated High Risk if it meets any of the following criteria:

1. Work involving functions or operations of the Department that are critical to the accomplishment of the mission of the Department;
2. Work involving investigative, compliance, or senior –level auditing duties;
3. Work involving fiduciary, public contact, or other duties involving the highest degree of public trust;
4. Personnel with IT security authority, "root" access to systems, or access to software source code have opportunity to bypass system security control settings i.e. network/systems administrator, system developer, and IT security program positions;
5. Any other work designated High Risk by the head of the OA or departmental office.

Moderate Risk – A contract will be designated Moderate Risk if it meets the following criteria:

1. Work involving free access and movement during normal work hours within a DOT facility which houses National Security information or equipment with little or no supervision by an appropriately cleared Federal Government employee;
2. Work occurring during restricted hours within a DOT facility which houses classified or sensitive information or equipment even though supervised by a Federal Government employee;
3. Work requiring access to sensitive information (information protected under the Privacy Act or Controlled Unclassified Information CUI);
4. "Super Users" of High or Moderate-impact systems who may modify core data stores, users with authority to electronically approve financial transactions, or users with access to personal/Privacy Act/ other protected data in it (e.g., social security numbers in human resource systems, etc.) other than their own. For these types of access privileges, the risk designation depends on the security categorization of the system involved.

Low Risk – Work that does not fall into any of the categories noted above will be given a Low Risk designation. For IT contracts, users with access to a DOC local area network, e-mail, basic office applications, and personal data records (i.e. only personal/private information pertaining to themselves such as their personal time and attendance record). For these types of access privileges, the risk designation depends upon the security categorization of the system(s) involved.