U.S. ARMY CONTRACTING COMMAND
REDSTONE ARSENAL (ACC-RSA)
REDSTONE ARSENAL, ALABAMA 35898

ACCESS CONTROL
STANDARD OPERATING PROCEDURE

12 December 2014

UNCLASSIFIED

TABLE OF CONTENTS

Title Page..... 1
Table of Contents..... 2
1. **General**..... 3
2. **Classification and Security**..... 3
3. **Location**..... 3
4. **ACC-RSA Mission**..... 3
5. **Objective/Purpose/Reference**..... 3
6. **Redstone Arsenal (RSA) Gate Access Procedures**..... 4
   a. Short Term Visitors (1-30 Days)..... 4
   b. Long Term Visitors (30-365 days)..... 5
   c. VIP Visitors..... 5
7. **ACC-RSA Building Access Procedures**..... 6
   a. Sparkman Center Access..... 6
      (1) Non-DoD Visitors with RSA Garrison Issued Badge..... 6
      (2) Military Retirees/Dependents..... 6
      (3) Non-DoD Visitors WITHOUT a RSA Garrison Issued Badge..... 6
      (4) Outside Door Access for Employees..... 6
   b. Bldg 5303..... 7
      (1) Non-DoD Visitors..... 7
      (2) Temporary DoD Visitors..... 7
      (3) Long-Term DoD Visitors..... 7
      (4) ACC-RSA Assigned Contractors/Non-DoD Personnel (GSA).... 7
      (5) New ACC-RSA Employees (Civilian/Military)..... 8
   c. Bldgs 7437/7442..... 8
   d. Bldg 7109..... 8
8. **ACC-RSA Protection/Security POCs**..... 8
9. **SOP POC**..... 8

ATTACHMENTS

A. RSA MAX System Access Form..... 9
B. RSA Long-Term Access Request Memo (30-365 Days)..... 10
C. SMO Access Request Memo..... 11
D. ACC-RSA Visitor Request Form..... 12

1. General:

a. Army Contracting Command- Redstone (ACC-RSA) designed its physical security programs to protect against the loss of Department of Defense (DoD) personnel, resources, and information due to criminal, terrorist, or hostile operations.

b. ACC-RSA Authority. The ACC-RSA Executive Director is the approving authority for permitting access for all personnel to ACC-RSA work areas and restricted areas; this authority has been delegated to the ACC-RSA Protection/Security Office. The ACC-RSA Protection Office, in conjunction with the Security Manager administers the access control program. All ACC-RSA assigned personnel will comply with this plan.

2. Classification and Security: This document, and its attachments, are unclassified and are approved for release as required to support the ACC-RSA access control program

3. Location: This SOP prescribes the access control measures to protect personnel, property, and information for all ACC-RSA facilities located in Huntsville, Alabama where ACC-RSA is primarily responsible for security. For the facilities where ACC-RSA personnel are tenants, and do not have the security lead, the ACC-RSA personnel will follow their host unit policies and procedures related to access control.

4. ACC-RSA Mission: Provide innovative, effective and efficient global contracting support to war fighters throughout the full spectrum of military operations.

5. Objective/Purpose/Reference: The ACC-RSA Protection Office designed this SOP to protect its personnel, resources and information from loss due to criminal, terrorist, or hostile actions. To accomplish this mandate, ACC-RSA must integrate all forces, devices and equipment into an effective security system, which complies with regulatory guidance set forth in the following references:

- AR 190-13, The Army Physical Security Program, 25 Feb 2011
- AR 190-51, Security of Unclassified Army Property, 30 Sep 1993
- AR 525-13, Antiterrorism, 11 Sep 2008
- AMC 525-13, AMC Force Protection Program, 6 Nov 2012
- RSA Installation Emergency Operations Plan 13-013, May 2013
- Sparkman Center Standard Operating Procedure, 4 Oct 2014
- Homeland Security Presidential Directive-12 (HSPD-12), 27 Aug 2004

6. Redstone Arsenal (RSA) Gate Access Procedures: The following steps outline the process for visitors that do not normally have access to RSA. For instructions on how to screen visitors for Bldg 5303, please see paragraph 7 below:

a. Short term visitors (1-30 days) that do not have DoD identification:

(1) At least ten working days prior to the scheduled visit, send the completed RSA MAX System form (Attachment A) to the Protection POCs in paragraph 8. Ensure the visitor includes their full SSN and the visit dates are accurately reflected on the form. ***Ensure the information is protected IAW PII requirements outlines in AR 340-21*** Recommend encrypted e-mail as the preferred method of sending PII.

(2) Upon receiving the completed form, the ACC-RSA Protection POC will enter the information into the RSA MAX System, which is linked, to the Federal Bureau of Investigation's National Crime Information Center (NCIC) system. A simple criminal background check will automatically be completed on the visitor by searching their SSN. This process can take up to 24 hours to complete. The visitor's status will be reflected as "pending" in the system until the NCIC check has been completed. Visitors whose NCIC check is completed favorably will be shown as "approved" in the MAX system and the ACC-RSA Protection POC will alert the visitor's sponsor that the visit request has been approved, the visitor may then go to the Gate 9 or Gate 1 RSA Visitor Control Center (VCC) to pick up their approved badge and enter the installation. This temporary badge will only be valid for the dates/times listed on the RSA MAX form. In the event that the NCIC check returns unfavorable results, the visitor will be flagged with an "alert" in the system. The ACC-RSA Protection POC may be able to mitigate the alert with the RSA visitor control personnel depending on the severity of the offense; this process may require additional information from the visitor. If the "alert" cannot be resolved, the visit request will be denied and the visitor's name and SSN will be added to the "denied list" for RSA; they will not be able to enter the installation until the situation is resolved with the RSA Police Department.

(3) The ACC-RSA sponsor is responsible for the visitor for the duration of the time that they are on the installation, this includes providing escort into any secure facilities, and taking steps to ensure the visitor does not, intentionally or unintentionally, view/receive controlled information (classified or unclassified). The visitor must also comply with all applicable RSA rules and regulations including, but not limited to, following all traffic laws, submitting to random/target searches conducted by security forces, and refraining from bringing prohibited items such as weapons on base. A list of prohibited items and local rules/laws are available at the RSA VCC for visitors or they may contact the RSA Police at (256)876-2222 for additional information.

(4) Upon completion of the visit, the visitor should drop off their temporary access badge at any of the RSA gates (there is a drop box with a slot on the outgoing lane nearest to the guardhouse at most gates). Visitors may also return the temporary badge to the ACC-RSA sponsor who will turn it into the ACC-RSA Protection representatives listed in paragraph 8. In the event the visitor does not drop off their badge, it will automatically expire and will no longer be valid past the visit date(s) listed on the badge.

(5) For repeat visits, follow the same steps above; however, if the NCIC check has been favorably completed in the previous 30 days, the system will automatically list the visit request as “approved”. The ACC-RSA Protection POC will relay to the approval to the ACC-RSA sponsor.

b. Long Term Visitors (more than 30-365 days):

(1) The ACC-RSA Deputy Directors may approve long-term visit requests for those vendors that require frequent contact with the contracting officers (KO) located on RSA. Each of the long term visitors will be screened in the same manner as listed above in paragraph 6.a.(2). The directorate requesting the long-term visitor badge will submit the MAX form (Attachment A) and the Long Term Visitor Request Memo (Attachment B) to the ACC-RSA Protection POCs listed in paragraph 8 below. Once the forms have been processed and the vendor has been properly screened with the FBI background check, the ACC-RSA Protection POC will alert the sponsor that the vendor may pick up their long-term badge at the gate 1 or Gate 9 Visitor Control Center. The ACC-RSA sponsor requesting the long-term aces for the vendor will be responsible for the vendor’s actions while they are on the Arsenal.

(2) 10 days prior to the expiration of the long-term badge, the above process will be repeated if continued access it required for the vendor. If the vendor does not require an renewal of their access, or the access is no longer required mid-way through their access term, the ACC-RSA sponsor will ensure the long-term badge is collected from the vendor and turned in to the ACC-RSA Protection POCs listed in paragraph 8 below for proper disposal.

(3) If the vendor loses track of their long-term badge and/or believe it has been stolen, the loss of the badge must be reported to the ACC-RSA Protection POCs immediately so that RSA Police may be alerted and the badge will be suspended in the tracking system until the matter is resolved.

c. VIP Visitors: Family members of ACC-RSA employees and/or high-ranking, non-DoD VIPs (local mayors, senators, etc…) that attend official gatherings (ACC-RSA Org Day, etc…) may be sponsored onto the base through the VIP request procedures. Please contact the ACC-RSA POCs listed in paragraph 8 for additional information. This method of sponsoring individuals onto RSA is restricted to specific events as the individuals will not receive the standard

background check, and they will not have to stop at either of the visitor control centers to enter RSA.

7. ACC-RSA Building Access Procedures: The following steps outline the process for visitors that do not normally have access to ACC-RSA controlled buildings on RSA:

a. Sparkman Center Access: The Sparkman Management Office (SMO) is responsible for the access control procedures/security for all external doors leading into the Sparkman Center. IAW the Sparkman Center SOP dated 6 Oct 2014; any RSA Garrison issued identification badge (RSA temp badges, RSA KE/ME badges), or the standard, government issued CAC/retiree/dependent ID card, is acceptable as identification to enter the Sparkman Center. All individuals in the Sparkman center are required to display their identification above the waist, on their outer most garment for the duration of the time they are in the center. Individuals that do not have an appropriate ID displayed should be challenged and reported to security.

(1) Non-DoD Visitors with a RSA Garrison Issued Badge: Vendors/visitors that have been issued a RSA temporary access badge may use that badge to enter the Sparkman Center through Bldg 5300 by signing in through security. The RSA badges cannot be programmed to open the other external doors in the Sparkman Center; visitors must process through security in Bldg 5300 OR be escorted by ACC-RSA personnel through the main doors of Bldg 5303.

(2) Military Retirees/Dependents: Individuals who retired from the military, or are military dependents with a military issued retiree/dependent ID card, may use that ID to enter the Sparkman Complex through Bldg security in Bldg 5300. The SMO security will issue the retiree/dependent a temporary SMO badge, which will be displayed IAW the procedures outlined above in paragraph 7.a.

(3) Non-DoD Visitors WITHOUT a Garrison Issued Badge: All vendors/visitors/family members visiting the Sparkman Center that HAVE NOT been issued a RSA Garrison Badge/CAC Card/military retired/dependent ID (therefore not having a FBI background check completed) are required to sign in with security in Bldg 5300 where they will receive a SMO Visitor's Badge. Their ACC-RSA sponsor must also escort the visitor(s) for the duration of the time they are in the complex.

(4) Outside Door Access for Employees: All personnel requiring temporary, or permanent, external door access into the Sparkman Center (through the doors with the card readers installed) will be required to process through the ACC-RSA Protection POCs listed in paragraph 8 below. Once the permission has been confirmed, the ACC-RSA Protection POC will submit the SMO Access Request Memo (see Attachment C) to the SMO Office for processing. Once the form is processed, the individual will go to the SMO Office window located near the elevators in Bldg 5300 to get their CAC card programmed. Those without

CAC cards will be handled on an individual, case-by-case basis as additional measures may be required to allow access.

b. Bldg 5303: The ACC-RSA Bldg located in the Sparkman Complex (Bldg 5303) is a RESTRICTED AREA that requires specific permissions for unescorted access. All doors/elevators entering the ACC-RSA areas of Bldg 5303 have card readers that are controlled internally by ACC-RSA Protection/Security.

(1) Non-DoD Visitors: ALL Non-DoD visitors to Bldg 5303 must be escorted at all times by their ACC-RSA sponsor. The escort will ensure the visitor(s) do not, intentionally or unintentionally, collect, overhear, or otherwise encounter restricted information such as proprietary information, contract award information, or any other form of controlled/restricted information (classified or unclassified). Each directorate sponsoring the visitor is responsible for the visitor while they are inside Bldg 5303. Non-DoD visitors can include vendors, family members, or anyone else that does not have an affiliation with a DoD agency and/or do not have a need to know the above, listed information.

(2) Temporary DoD Visitors (visits less than five days): All DoD visitors from non ACC-RSA agencies will be escorted while they are in Bldg 5303 unless arrangements have been made IAW the next paragraph.

(3) Long-Term DoD Visitors (visits of five days or more): IAW AR 190-13, only screened persons that have had a favorable background check can be granted unescorted status within a restricted area. The Protection Officer or the Security Manager can verify the favorable background check in the Joint Personal Adjudication System (JPAS) for the DoD visitor; the visitor will be required to provide their full Social Security Number (SSN). The ACC-RSA sponsor for the long-term DoD visitor will do the following:

(a) Complete the ACC-RSA Visitor Access Form (see Attachment D); at least 10 days prior to the visit, submit the completed form (sections one and two filled out) to the Protection POCs in paragraph 8 below.

(b) Ensure the DoD visitor's Security Manager submits a visitor access request through JPAS IAW the instructions at the top of Attachment D.

(c) Once the background check has been verified the visitor's access form will be processed and the visitor's CAC card will be approved to be programmed to access to the doors/elevators within Bldg 5303 as specified on the form. The visitor will not require an escort during the duration of their visit.

(4) ACC-RSA Assigned Contractors/Non-DoD Personnel: Individuals that are hired or appointed to support ACC-RSA by working in Bldg 5303 (contractors, GSA employees, etc…) will be required to obtain a DoD CAC card through the trusted agent program. Mr. Ken Purdin is the trusted agent for ACC-RSA; contact Mr. Purdin for the procedures and requirements. Once the

individual has a DoD CAC card, follow the instructions listed in the "Long-Term DoD Visitors" paragraph above to have the CAC card programmed to access Bldg 5303.

(5) New ACC-RSA Employees (Military and Civilian): Newcomers will in-process the Protection and Security Offices of ACC-RSA as part of their initial orientation, their security information and CAC card programming will occur as part of the standard in processing procedure.

c. Bldgs 7437/7442: Follow the same procedures listed above for Bldg 5303.

d. Bldg 7109: Contact Mr. Charles Looney, Security Manager at (256) 955-0260 or charles.e.looney8.civ@mail.mil.

8. ACC-RSA Protection/Security POCs:

a. Primary: Mr. Ken Purdin
ACC-RSA Protection Officer
Bldg 5303, 3rd Floor, Room # 3326
(256)955-9336
Kenneth.r.purdin.civ@mail.mil

b. Alternate: Mr. Rich Sherman
ACC-RSA Security Manager
Bldg 5303, 3rd Floor, Room # 3326
(256)842-9245
richard.a.sherman24.civ@mail.mil

c. Alternate: Mr. Randall Bunley
ACC-RSA Operations
Bldg 5303, 3rd Floor
(256)955-6136
randall.c.bunley.civ@mail.mil

9. SOP POC: The POC for this SOP is the ACC-RSA Protection Officer, Mr. Ken Purdin; the contact information is listed above in paragraph 8.

CRISTINA G. RODRIGUEZ
Deputy Director, Business Management
Directorate-Resources
Army Contracting Command-Redstone

Attachment A
RSA MAX Access Form

MAX System Information

RSA Access

SSN	Name		
Primary Citizenship		Indicate Dual Citizenship	
Address	Organization/Company		Office Symbol
.			
City	Grade/Rank	Person Type	
.		N/A	
State	Position Title	Clearance	
.			
ZIP	Home Phone	Duty Phone	
.	.		
Hair Color	Eye Color	Height (in)	Weight
.	.	.	.
DOB	Sex	Race	Birthplace
.	.	.	.
Drivers License	State of Issue	.	Person Status
.	.	.	.N/A
Email Address		.	
		.	
Remarks			.

Attachment B
RSA Long-Term Access Request Form (30-365 Days)

DEPARTMENT OF THE ARMY
ARMY CONTRACTING COMMAND - REDSTONE
BUILDING 5303 MARTIN ROAD
REDSTONE ARSENAL AL 35898-5000

CCAM-BMS DATE: _____

MEMORANDUM FOR ACC-RSA PROTECTION/SECURITY

SUBJECT: RSA Long-Term Access Request for Non-DoD Personnel

1. The _____ Directorate requests the following non-DoD vendor be issued a long-term RSA access badge for _____(30-365) days so that they may conduct frequent and official business with ACC-RSA assigned employees located on Redstone Arsenal. The vendor listed below is expected to come onto RSA to conduct official business _____ times a **week/month** (circle one) starting on _____ (date) and ending on _____ (date).

2. Sponsored Vendor:
   Name:_____
   Company:_____
   Phone/E-Mail:_____

***Please ensure a RSA MAX System Information Form is attached for the above individual with their full SSN listed** A background check will be conducted IAW standing policy.

3. ACC-RSA Sponsor:

   I understand that I will be responsible for the actions of the above listed individual while he/she is on RSA and I will be responsible to provide an escort when he/she is required to enter any restricted/secure locations on post.

   _____ _____
   Printed Name Signature

   _____ _____
   Office Symbol Phone

4. ACC-RSA Deputy Director approval:

   I have reviewed and approve the request to issue the individual listed in paragraph 2 a long-term RSA gate access badge to conduct official business with ACC-RSA personnel assigned to my directorate. I understand my directorate is responsible for the visitor while he/she is on Redstone Arsenal.

XXXXXXXXXXXXX
ACC-RSA Deputy Director

Attachment C
SMO Access Request Memo

DEPARTMENT OF THE ARMY
ARMY CONTRACTING COMMAND - REDSTONE
BUILDING 5303 MARTIN ROAD
REDSTONE ARSENAL AL 35898-5000

CCAM-BMS DATE: XXXXXXXX

MEMORANDUM FOR SPARKMAN MANAGEMENT OFFICE

SUBJECT: Issuance of Sparkman Center Building Access

1. Request Sparkman Center access be granted to the below listed individual for entry into Bldg 5300.

2. Employee Information:

Full Name: XXXXXXXXXXXXXXX

Employee Type (Check one): **Government:**_____
Contractor:_____

Access Type (Check one): **General Access** (0500-1900, M-F)_____
After Hours (24/7)_____

Work Phone Number: XXXXXXXXX

3. The undersigned approves access to Bldg 5303 for the employee; all applicable security checks and measures have been completed IAW standing orders and the Sparkman Center Building Access SOP.

5. Point of contact is the undersigned at (256) 955-9336 or email: kenneth.r.purdin.civ@mail.mil.

KENNETH R. PURDIN
ACC Protection Officer

Attachment D
ACC-RSA Visitor Request Form

DIRECTIONS:
1) Tell the visitor to process a Visit Access Request (VAR) through their security officer to BLDG 5303, ACC-RSA, using SMO Code W6QK1A and complete #1 and #2 below.

2) E-Mail the form to richard.a.sherman24.civ@mail.mil.

3) For visits to BLDG 5303 less than once a month on average, ACC-RSA personnel must escort visitors rather than request independent access.

ACC-REDSTONE Access Request

1. VISITOR INFORMATION:

NAME: First _____ Middle Init ____ Last _____

PHONE _____ E-MAIL _____

COMPANY _____SUPERVISOR _____

SUPERVISOR E-MAIL _____

REQUESTED DATES AND TIMES FOR ACCESS TO BLDG 5303:

_____

2. SPONSOR INFORMATION (BLDG 5303 PERSONNEL):

BLDG 5303 SPONSOR NAME _____ PHONE _____

ALTERNATE SPONSOR NAME _____ PHONE _____

3. VISITOR ACCESS REQUEST (VAR)(THE ACC-RSA SMO CODE IS W6QK1A):

NOTE: This section to be completed ACC-RSA security personnel and routed to the BLDG 5303 sponsor.

VAR verified in JPAS ☐ Hard Copy ☐ Approved through: Day ____ Month ____Year _____

VAR Certifying Official: _____Date: _____

4. ACC-RSA SPONSOR STATEMENT VALIDATING NEED FOR ACCESS:

Note: To get access, the sponsor or their designee will escort the visitor to see Katie Clark, 3rd floor BLDG 5303. The visitor must have this completed form and their CAC card if they are a CAC holder.

This visitor needs access to (place an X for each floor): Hallway only First ☐ Second ☐ Third ☐ I certify that the visitor above has a valid need for access to BLDG 5303 for the period stated above. The VAR has been confirmed for CAC holder visitors. If the visitor is a NON-CAC holder, I have informed the visitor that the swipe card must be returned after expiration of the access period.

Sponsor Signature: _____ Date: _____