Department Of Defense
ALL-HAZARDS THREAT ASSESSMENT (2020)
USAG-Redstone

(U) DTG: 060900JUN2020

(U) Subject: All-Hazard Threat Assessment for Redstone Arsenal

(U) Information collection cutoff date: 4 February 2020

(U) The following observations were derived from the 2019 RSA Threat-Hazard Risk Assessment:

(U/FOUO) Most Likely Course of Action: (Cyber Attack). The Installation Threat Working Group determined that a Cyber Attack has the highest probability from an all hazards threat perspective. The most plausible scenario is a person conducting unauthorized access to a control system device and/or network using a data communications pathway from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders. The potential for a Cyber Attack is very high.

(U) Most Dangerous Course of Action: **(Tornado Event).** The Installation Threat Working Group determined that the highest severity would be derived from a tornado event. The most plausible scenario is an (F3) Tornado touching down on RSA traveling from the southwest corner of the installation to the northeast corner damaging facilities and infrastructure.

(U) Highest Residual Risk: (Tornado Event). A tornado event is the number one threat/hazard based on the overall probability and severity. In the past several touchdowns have occurred on RSA causing property and structure damage. Due to the known and potential severe weather pattern of the local area and the fact that surrounding communities have suffered exceptional loss of property and life.

(U/FOUO) Design Basis Threat (DBT): Redstone Arsenal is designated a controlled perimeter Installation with established access control measures. The area outside of the Installation's perimeter is considered the uncontrolled perimeter. The current Design Basis Threat for RSA is as follows:

A. (U/FOUO) Controlled Perimeter:

A.1. (U/FOUO) **220lbs (TNT equivalent).** A bomb weighing up to 220lbs could be smuggled onto USAG-R in a vehicle, provided the driver possessed legitimate access to the Installation (Legitimate CAC card or military identification). The threat for a vetted person bringing this type of IED on the post is considered

LOW. Additionally, it is very difficult for individuals to obtain the materials necessary to construct a bomb of this size.

A.2. (U/FOUO) 55lb (TNT equivalent) improvised explosive device (IED). This is the Installations current Design Basis Threat for facilities. A 55lb Improvised Explosive Device (IED) could be delivered on post undetected, so therefore facilities are designed to meet the minimum AT construction requirements IAW UFC 04-010-01 and UFC 04-010-02. Numerous large packages arrive on a daily basis. It is significantly easier to conceal a bomb in these larger packages, particularly if the packages appear to originate from a legitimate business. If such packages bear legitimate markings, appear to be shipped from a legitimate company and are accompanied by legitimate bills of lading, it is possible that it would reach its intended destination without additional screening or inspections with explosive detection canines. The threat of vetted persons such as (RSA employees or persons with a sponsored visitor badge) bringing a IED on post undetected is considered HIGH as they may not be subject to a vehicle RAM inspection yet the probability is LOW. Persons with a recreation badge would have a higher probability of detection due to their increased vehicle inspection requirements.

A.3. (U/FOUO) **Mail 2lbs IED**. USAG-R is vulnerable to a mailed bomb, although screening features at the USAG-R mail center could detect a mailed bomb that was not marked properly or that displayed evidence of an enclosed bomb (discolored wrapping paper, improper addressing, unordinary odors, etc.). Although packages addressed to senior personnel are screened at multiple levels, a well-disguised and properly addressed mail bomb could reach its intended destination.

B. (U/FOUO) Uncontrolled Perimeter: **550lbs or greater (TNT equivalent).** Bombs this size are difficult to conceal and the possibility of a vehicle parking near DoD assets along the Installations perimeter undetected is unlikely. All commercial delivery vehicles entering RSA are searched for possible explosive devices and vetted personnel and visitors are subject to RAM inspections. Commercial delivery vehicles have a **LOW** potential of successfully delivering a large IED on post undetected. Additionally, it is very difficult for individuals to obtain the materials necessary to construct such large bombs, although it is not an entirely unattainable goal. Based on the difficulties to acquire such a large quantity of explosives, the threat for vetted personnel or visitors to bring this type of IED on the post is considered **Very LOW**.

(U/FOUO) All Hazard Threat Matrix: The following threats and hazards were prioritized by the Installations Threat Working Group and approved by the Garrison Commander. Each undesirable event was prioritized by multiplying their probability X severity in order to establish the overall threat/hazard rankings.

Threat-Hazard Matrix (priority)	Undesirable event	Likely Scenario
(1)	**Tornado (seasonal March – August timeframe)**	A (F3) Tornado touches down on RSA traveling from the southwest corner of the installation to the northeast corner damaging facilities and infrastructure.
(2)	**Foreign Intelligence Entity (FIE)**	Malicious actors targeting multiple organizations affiliated with the defense industry in the vicinity of Huntsville, Alabama. Foreign collectors obtain illegal or unauthorized access to sensitive or classified information and technology.
(3)	**Cyber Attack (Cyber Terrorism)**	Persons conduct unauthorized access to a control system device and/or network using a data communications pathway from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders.
4	**Aircraft/Airfield Accident (Non Terrorism)**	A fixed or rotary wing aircraft make a crash landing on RSA's airfield.
5	**Active Assailant**	A person enters asset and begins to assault occupants.
6	**Range/Test Area Explosion**	An accidental explosion takes place in one of RSA's Test Area during testing.
7	**Unmanned Aerial System (UAS) with IED**	A UAS with explosive payload equivalent to 15 lbs. TNT is launched close to the installations perimeter. It then flies to an open air special event and releases its cargo over a mass populated area.
8	**Biological: Disease Outbreak (PI)**	A Pandemic event occurs impacting Redstone Arsenal operations.
9	**Explosive Device (Terrorism)-Mailed or Delivered**	An explosive device is sent to a facility through U.S. Mail or a commercial delivery service, including an unwitting courier.
10	**Chemical: Release of a chemical agent filled munition or container**	An accidental explosion or mechanical breach of a munition or container, resulting in a chemical release and plume traveling through populated areas both on and off installation.
11	**Chemical: TIC/TIM spill**	A vehicle transporting a TIC/TIM has an accident in the vicinity of RSA causing the TIC or TIM to leak. The plume of the TIC/TIM travels through populated areas.
12	**Adverse Winter Weather**	A winter storm hits RSA causing slippery road conditions around bridges and overpasses to include busted water pipes, broken power lines and downed tree branches.
13	**CBR Release (Terrorism) –Food/ Water Supply**	An individual deliberately contaminates food, drinking source or water supply during a large scale special event.
14	**Wild Fire**	A wild fire starts on a Range or Test Area spreading throughout the vicinity causing minor damage to facilities or infrastructure.
15	**Explosive Device (Terrorism) – VBIED**	A mid-size vehicle packed with 55lbs of plastic explosives parks next to a mass gathering facility or area then detonates.
16	**Civil Disturbance**	A deliberate and planned demonstration is held outside the Redstone Arsenal perimeter erupting with acts of violence towards military and DoD personnel.

17	**Chemical: Release of Onsite Hazardous Materials**	A person with unauthorized access to hazardous materials stored onsite releases materials with the intent of harming personnel or damaging the facility.
18	**Theft Robbery**	Unauthorized taking of Government-owned or personal property from an employee or other person(s) by force or threat of force. The incident could occur inside or outside of a facility.
19	**CBR Release (Terrorism) High population facility/ area**	An Intentional release of a CBR agent is released in the vicinity of a mass population facility through a specific access point, such as air intake, windows, or doorways, from outside the facility.
20	**Flooding**	Severe weather causes a flash flood on RSA. The floods impact the recreation areas and disrupt traffic flow on a small number of roads.
21	**Radiological: Power Plant/ Nuclear Reactor incident**	Browns Ferry Nuclear plant has a radiological release cased triggered from a large scale tornado or earthquake.
22	**Earthquake**	An earthquake erupts in northern Alabama damaging facilities and infrastructure.

1. (U) Executive Summary: The results of this assessment serves as a baseline for the Threat Working Group's (TWG) continual process of compiling and examining available information concerning potential threats and hazards. This assessment reviewed an all hazard threat spectrum against Redstone Arsenal (RSA) personnel and facilities. Terrorist Threat Levels are categorized as *LOW, MODERATE, SIGNIFICANT*, and *HIGH*. Additionally, the TWG evaluates "Risk" associated with each Threat or Hazard. Risk levels are categorized as *LOW, MODERATE, HIGH* and *VERY HIGH*. A complete Risk Assessment can be found in the installations annual threat/hazard Risk Assessment.

The Redstone Arsenal all hazard/threat assessment addresses the entire threat/hazard spectrum with emphasis on specific events and related capabilities within our geographical area. This data is provided for Redstone Arsenal units and activities in order to assist with developing local exercise scenarios, criticality assessments, vulnerability assessments, risk assessments, to include Antiterrorism and Physical Security Planning and AT/FP construction requirements.

1.A. (U/FOUO) Terrorist Threat. The terrorist threat level for Redstone Arsenal is ***MODERATE.*** The DIA Continental United States (CONUS) Threat Assessment is ***SIGNIFICANT.*** A US person was arrested in Huntsville Alabama on 15 June 2017 for soliciting or providing support for an act of terrorism. The arrest was the result of a tip from a local citizen.

1.B. (U/FOUO) Foreign Intelligence Entity (FIE) Threats.
The FIE threat to Redstone Arsenal is considered a ***HIGH risk*** due to consistent incident reporting of malicious actors targeting multiple organizations affiliated with the defense industry in the vicinity of Huntsville, Alabama. Over the past decade, the total number of industry reports concerning attempts by foreign collectors to obtain illegal or unauthorized access to sensitive or classified information and technology continues to rise, with East Asia, and the Pacific regions being the originators of almost half of the incidents. Based on trends in suspicious contact reporting, these foreign actors utilize methods to include suspicious network activities, attempted acquisition of technology, and direct requests for information. While commercial collectors remain the most common mechanism to collect data, the use of government-affiliated entities still remains a contender in a portion of procurement attempts.

1.C. (U) Crime. The criminal threat to RSA is considered ***LOW risk.*** The Redstone Arsenal CID and LE reviews crime data regularly in order to maintain current assessments of the criminal threats to RSA and the surrounding area.

1.D. (U/FOUO) Civil Disturbance. This threat is considered ***LOW risk.*** Although demonstrations have been traditionally small outside the post, the potential for larger demonstrations exist depending on military operations and

Overseas Contingency Operations. The factors supporting the threat assessment are existence, capability and history.

1.E. (U/FOUO) Medical. The overall medical/health/safety to the geographical area is assessed as a ***LOW risk***. Although there are a few low community risk outbreaks within the US, currently there are no significant or potential high risk health activities noted CONUS. This assessment may change in the future if significant health activities are noted. The medical community continues to watch and assess for ZIKA and Influenza. Both health activities continue to be low within this AO. Food-borne outbreaks are a moderate threat, as these outbreaks can and do occur sporadically.

1.F. (U/FOUO) Cyber. The International Cyber Threat to the Information Systems (IS) on Redstone Arsenal is assessed as a ***HIGH risk.*** A new title has been associated with cleverly engineered collection techniques; Advanced Persistent Threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity. Open sources equate APT to target organizations and/or nations who hack/attack for business, financial or political motives.

1.G. (U) Natural Hazards. RSA has assessed the severe weather threat as a ***MODERATE risk***. The primary weather threats to RSA are tornadoes, thunderstorms, and their associated effects.

1.H. (U/FOUO) WMD. The Force Protection and Installation Emergency Management Working Groups assess the overall WMD/CBRN threat to RSA as a ***LOW risk.*** The threat to the installation posed by Toxic Industrial Materials (TIM) cannot be dismissed since an accident or attack could occur at any time and location. The most probable incident is using a rail-tanker or other motor vehicle transporting toxic industrial chemicals (TICs are subsets of TIMs). This could be either an accidental or a terrorist detonated incident at such a time and place so as to disperse a poisonous gas plume over selected areas of RSA. Locally available ammonium nitrate (fertilizer), anhydrous ammonia and chlorine are homeland security concerns because of their properties and availability. They are especially hazardous because the ammonium nitrate when mixed with fuel oil will produce an explosion similar to the Oklahoma City bombing.

1.I. (U) Safety. Safety is the number one concern for the RSA workforce. Risk Assessments are completed for all special events and mission operations.

1.J. (U/FOUO) Security. Redstone Arsenal is considered a "Closed Installation/Perimeter." The installation perimeter is protected by security fencing or natural barriers such as the Tennessee River, other wetlands and steep cliffs. Installation access is controlled by Department of the Army Civilian Security Guards under the supervision of the Directorate of Operations (Protection Division). ACPs have been renovated with state of the art equipment to preclude

unauthorized entry. All ACPs are equipped with Ground Retractable Automobile Barriers (GRAB) to prevent forced entry. A commercial vehicle inspection area is located at ACP#1. Visitor Control Centers are located at the installation perimeter adjacent to ACP#1 and 9. The visitor control centers verify personnel requirements for access and issue credentials for visitors, contractors, foreign nationals, mission essential personnel and security areas. A National Criminal Information Check (NCIC III) is currently conducted on all contractors, foreign nationals and visitors. All "Official Mail" is screened at the Redstone Post Office. The installation does not employ a central receiving and distribution point for all deliveries. Vendors such as UPS, FedEx, and the USPS deliver packages and supplies directly to customers on Redstone Arsenal. Vehicle RAM is conducted daily.

1.K. (U/FOUO)Toxic Industrial Chemicals/Toxic Industrial Materials (TICS/TIMS). Although the Threat Working Group assesses the overall "WMD" threat to Redstone Arsenal as a ***LOW risk***, the threat to the installation posed by Toxic Industrial Materials (TIM) Or Toxic Industrial Chemicals (TIC) is assessed as a ***MODERATE risk***.

1.L. (U) Malicious/Insider Threat. RSA has assessed its Malicious/Insider Threat as a ***MODERATE risk***. The malicious/Insider threat comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, sabotage of computer systems or active shooter events.

1.L1. (U) Insiders may have accounts giving them legitimate access to computer systems, with this access originally having been given to them to serve in the performance of their duties; these permissions could be abused to harm the organization. Insiders are often familiar with the organization's data and intellectual property as well as the methods that are in place to protect them. This makes it easier for the insider to circumvent any security controls of which they are aware. Physical proximity to data means that the insider does not need to hack into the organizational network through the outer perimeter by traversing firewalls; rather they are in the building already, often with direct access to the organization's internal network. Insider threats are harder to defend against than attacks from outsiders, since the insider already has legitimate access to the organization's information and assets

1.L.2. (U) The motivation for individuals associated with insider threats can be attributed to greed or financial need, being angry or disgruntled, dissatisfaction or disagreements with work or co-workers, divided loyalty, or misdirected ideologies, among other things. Specific organizational shortcomings can further exacerbate the potential for an insider threat by providing access privileges to individuals who do not necessarily require them, not properly protecting sensitive

or classified materials, undefined or nonexistent document handling requirements and enforcement, perceived lack of a security program, or improperly trained employees.

1.L.3. (U) Leaders, supervisors, and co-workers must be aware of outsiders who may try to formulate some sort of relationship with those who have access to the Post. Some may try to recruit like-minded individuals for the purpose of criminal or terrorist acts.

1.M. (U/FOUO) Food/Water Contamination Threat. Food/Water Contamination Threat. The overall food/water contamination threat is a ***LOW risk***. A concern for special events may be the provision of food from unapproved sources. These foods may be produced under unsanitary conditions, further processed under unsanitary conditions, or may be at risk for intentional as well as unintentional contamination. Controls to reduce risk are in place, and include food vulnerability assessments in addition to sanitary inspections conducted prior to these events, in addition to oversight of food preparation by preventative medicine and veterinary services. An additional concern is the oversight of food truck vendors on temporary contracts. Permanent contracts allow for electronic tracking of sanitary inspections, approved source verification, as well as food vulnerability assessments, while temporary contracts rely solely on regular communication of contractors with Preventative Medicine and Veterinary Services to ensure proper inspections are completed.

1.N. (U/FOUO) Local Gang Activity: The threat of gang violence is considered a ***LOW risk.***

1.N.1 (U/FOUO) Street Gangs: Currently the most active "Street Gang" in the Huntsville area is the "Goon Squad Mafia" (GSM). This gang is a member of the "Bloods Set". Other gangs include:

1.N.1.A. (U) Gangster disciples

1.N.1.B. (U) Bloods

1.N.1.C. (U) Crips

1.N.1.D. (U) MS-13

1.N.2. (U/FOUO) Outlaw Motorcycle Gangs (OMG): OMG's known to operate in the area are "Outcast, The "Saints" and "Iron Coffin M/C. Alabama is also known to have a presence of "The Bandidos" as well as "Pagans". Motorcycle clubs are known to attract former military members, including retirees. Primary concern would be with "support clubs", Motorcycle clubs that are affiliated with an OMG, but not classified as an OMG. The support clubs are the primary means OMGs use to recruit new members. Although the threat is low on the Arsenal, it is not

hard for any off post occurrence to migrate on to the installation and cause the LE team to respond.

2. (U/FOUO) Terrorist Threat. There are general threats directed toward U.S. military, law enforcement, and the American public. The most likely attack would generate from Homegrown Violent Extremist (HVES) and lone offenders using simple means of attack such as small arms, edged weapons, and possibly simple IEDS. ARTIC is concerned that HVES and lone offenders may be influenced by recent attacks. Violent extremists view military personnel and installations, both overseas and The US, as attractive targets, which raises security concerns. Military installations may have multiple levels of security, based upon the types of assets located on the base, as well as the number of military personnel, civilians, government employees, contractors, retirees, and their families. The tenants of a military installation may also vary depending on the physical location, mission set, and mutual security and property agreements between US Government and local authorities. Entry requirements for employees, residents, and visitors may vary between installations making some locations easier for violent extremists to gain access to than others. In addition, the range of tenants within the military installation and the possibility of multiple jurisdictions surrounding a military installation may complicate emergency calls for service. The exclusive federal jurisdiction on a military installation may present challenges when responding to a terrorist attack which requires the assistance of state, local, tribal, and territorial first responders, if cooperative plans, training, and exercises are not set into place.

A. (U/FOUO) Possible Terrorist Targets:

Economic	Banking/Federal Reserve/Mint
Military	Military Installations
Political	State/Local Monuments
Infrastructure	Power Plants Dams/Water Supplies Bridges Road/Rail Network Airports
American Life Style	Entertainment Industry Sporting Events Shopping centers Schools/Churches

B. (U/FOUO) Extremists / Hate Bias Groups: This threat is considered a ***LOW risk.***

C. (U/FOUO) Summary of Single issue groups in our AOR: FBI and DHS assess on the basis of recent and historical incidents that violence by **domestic extremists** will likely include numerous assaults, several shooting incidents per

year, and several incidents over the next four years involving improvised explosive devices (IEDs) or improvised incendiary devices intended to result in multiple casualties or significant property losses.

3. (U/FOUO) Foreign Intelligence Entity (FIE)
The foreign intelligence entity threat to Redstone Arsenal is ongoing and uses the multi-faceted threats of HUMINT, IMINT, SIGINT, and OSINT in its collection operations against the installation. The collection effort targeted against the personnel of this installation typically includes:

3.A (U) Request for information

3.B. (U) Solicitation and marketing of services

3.C. (U) Attempted acquisition of US technology

3.D. (U) Exploitation of foreign visits

3.E. (U) Exploitation of existing relationships

3.F. (U) Internet activity "hacking"

3.G. (U) Targeting at conventions

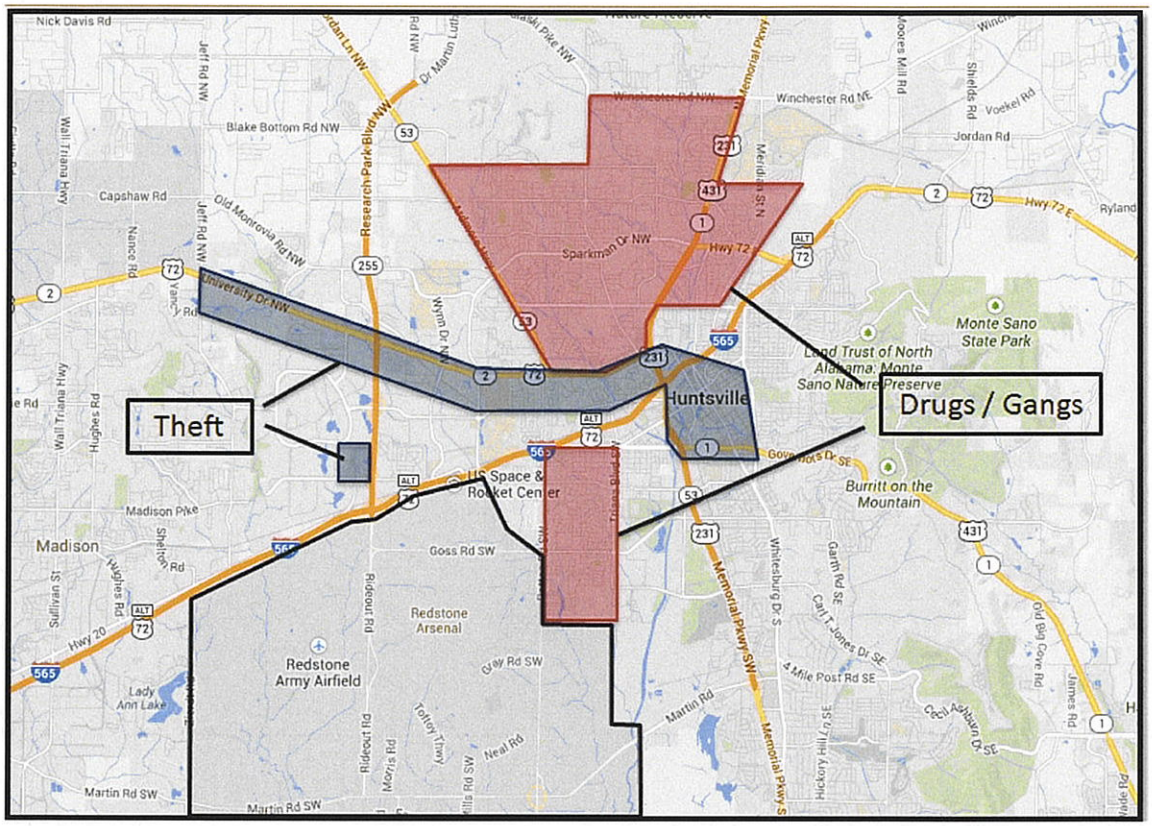
4. (U) Crime. Crime levels surrounding Redstone Arsenal are similar to those found in cities of comparable size. The primary criminal threat on RSA is petty theft of valuables left unsecured or in plain view. Additional threats include minor traffic accidents due to speed and inattentive driving. In the surrounding community, the primary threat to event attendees would also be petty theft. Open source crime trends do not indicate an increase in violent crime types impacting RSA personnel.

4.A. (U) At A Glance/2019 Crime Statistics (Huntsville PD):

Reported Crime:	2018	2019	Trend 2018-2019
Homicide	29	19	34% Decrease
Forcible Rape	164	162	1% Decrease
Robbery	325	307	6% Decrease
Burglary	1,361	1,193	12% Decrease
Larceny Theft	6,621	5,811	12% Decrease
Motor Vehicle Theft	1,106	925	16% Decrease

Unlawful B&E	1,809	1,405	22% Decrease
Simple Assaults	5,326	5,239	2% Decrease
Arson	25	16	36% Decrease

4.B. (U) Elevated Crime Areas:



5. (U/FOUO) Civil Disturbance. No protest or civil disturbance events were reported in the vicinity of Redstone Arsenal for CY2019. One protest was conducted in the vicinity of Gate 9 on 7 April 2017. The protest supported the 25th Annual Space Organizing Conference. The protest/demonstration was peaceful and went off with little impact to the Installation. USAG-R recorded around 42 protestors, 8 vehicles and one motorcycle in all.

6. (U/FOUO) Medical/Health. There are normally a few low community risk outbreaks within the US; currently influenza is widespread across throughout CONUS. This assessment may change in the future as flu activity dissipates or increases. The medical community continues to watch and assess for ZIKA, seasonally; Zika threat continues to be low within this AO. Food-borne outbreaks are a moderate threat, as these outbreaks can and do occur sporadically.

7. (U/FOUO) Cyber Threat. The importance of protecting the Department of Defense Information Network (DoDIN) from entities with nefarious intentions has become even more paramount predicated on our government's continued reliance on automation and connected systems. This trend has expanded our threat vector, creating a more expansive target for those entities wanting to negatively affect government systems that support the warfighter. The robustness of computing capabilities that are easily available to hackers, coupled with the sharing of information and widespread availability of hacking practices creates even greater challenges when trying to protect DoDIN assets against cyber threats. Over the past 12 months, there have been several critical threats associated with Army Networks; Supply-Chain, Misconfigured Network Devices, Access Controls, Program of Record systems, Commercial Application Networks, U.S. Army Network Modernization, and Mobile Devices.

7.A. (U/FOUO) Supply-Chain.
Threat actors have been able to garner access to U.S. Army supply chains in order to deny, degrade, disrupt, destroy, or exploit U.S. Army networks and data. This is made possible through the use of decentralized accounting, administration, and procurement of network devices and software.

7.B. (U/FOUO) Misconfigured Network Devices.
Threat actors have garnered unauthorized access to U.S. Army network devices and data in order to exploit weaknesses. Vectors for entry include printers, public facing web servers, proxy servers, teleconferencing equipment, firewalls, routers, and switches.

7.C. (U/FOUO) Access Control.
Threat actors are able to exploit information systems or resident data, either physically or logically, in order to bypass defense-in-depth mechanisms. This exploitation is made possible by compromising an individual's elevated account privileges or by gaining physical access to network infrastructure devices through social engineering techniques.

7.D. (U/FOUO) Program of Record Systems.
Threat actors are able to garner access to special use networks or systems, such as Program of Record systems through the exploitation of unpatched vulnerabilities within legacy applications or operating systems. In doing so, the threat actors are able to gain entry into U.S. Army networks and data. This occurs because most special systems are exempt from following normal patch cycles but are still allowed to connect to U.S. Army networks.

7.E. (U/FOUO) Commercial Network Applications and Services.
Threat actors are able to gain access to U.S. Army networks and government and military personally identifiable information through the utilization of social engineering and susceptible commercial sites such as Facebook, LinkedIn, and personal email accounts.

7.F. (U/FOUO) U.S. Army Network Modernization.
Threat actors are able to exploit U.S. Army network modernization initiatives such as advanced routing protocols, IPv6 transition, and Public Key Infrastructure due to the hardware and software implementations that are required to achieve the desired results. Additionally, the gaps between transition periods create a static compliance window that weakens the U.S. Army networks security posture.

7.G. (U/FOUO) Mobile Devices.
Threat actors are able to infect mobile devices through such acts as Bluetooth hacking and wireless session interception. In doing so, threat actors are able to utilize listening and recording devices to exploit sensitive or classified data that may be openly discussed or displayed.

7.H. (U/FOUO) The Installation's Cybersecurity Defense in Depth posture has prevented many attempted attack sessions. On average, the Redstone NEC Cybersecurity Division reviews over 50,000 lines of potential malicious attacks per week. To help combat malicious software threats, the Cybersecurity Division has emphasized computer security and user-level training through Newcomers Briefings, Security Managers Course, Cyber Awareness Challenge, Information Management Officers Course, Information Assurance Fundamentals course, OPSEC and TARP presentations. Although many view the Acceptable Use Policy as a way to impose restrictions, its true purpose is to protect the employee and the ICAN. Inappropriate use exposes the Redstone Arsenal networks to various risks and compromise of network systems and services.

8. (U) Natural Hazards. Tornadoes are the most significant weather threat to RSA facilities and/or personnel, particularly March through May, which is peak tornado season in the Southern states, a secondary tornado season can occur in the fall, typically in November. Compared with other states and based on National Weather data from 1950 - 2015, revealed that Madison County, Alabama had over 139 "reported" tornadoes. Twenty-three (33%) were rated with an intensity of F-2 (113-157mph) or above. This figure is an interesting contrast to the national average, in which 88 percent of all tornadoes are rated with winds below the F-2 level. On 27 April 2011, a significantly powerful storm system impacted the Southeast Region. Huntsville experienced three separate waves of severe weather that day. The storm system included multiple EF5 and EF4 tornadoes, resulting in 242 deaths and 2,187 injuries in Alabama alone. Seven of those tornadoes took place in Madison County with 9 deaths reported (injuries were not noted) Tornadoes are the most likely threat to cause a mass casualty event on RSA.

Floods are occasional threats to RSA's southern border, which is defined by the Tennessee River. However, floods along RSA more often tend to result in property damages rather than loss of life. Floods similar to tornadoes and severe

thunderstorms, tend to generally occur most frequently during the late winter and spring, but can develop at any time of the year when conditions are right. The National Weather Service monitors the flood stage of larger streams which could overflow their banks, affecting the residents of Madison County. In Madison County, these streams are the Tennessee River, the Paint Rock River, the Flint River, and Indian Creek. Flooding can be divided into two categories: flash floods and mainstream flooding.

During the colder winter months, the Tennessee Valley can sometimes experience cold fronts that send artic air from Canada southward into the region. These can send temperatures well below freezing and in some cases below zero as well. Given the right ingredients, such as deep moisture, winter weather can develop and impact the area in the form of snow, sleet or freezing rain.

9. (U/FOUO) Weapons of Mass Destruction (WMD). Terrorist could use an explosive device, a TIM, and/or radiological dispersal device near key infrastructure/ mission essential facility to inflict terror and chaos regardless of success of attack. The threat to the installation posed by Toxic Industrial Materials (TIM) cannot be dismissed since an accident or attack could occur at any time and location. The most probable incident is using a rail-tanker or other motor vehicle transporting toxic industrial chemicals (TICs are subsets of TIMs). This could be either an accidental or a terrorist detonated incident at such a time and place so as to disperse a poisonous gas plume over selected areas of RSA. Locally available ammonium nitrate (fertilizer), anhydrous ammonia and chlorine are homeland security concerns because of their properties and availability. They are especially hazardous because the ammonium nitrate when mixed with fuel oil will produce an explosion similar to the Oklahoma City bombing.

10. (U) Safety. Safety is the number one concern for the RSA workforce. Risk Assessments are completed for all special events and mission operations.

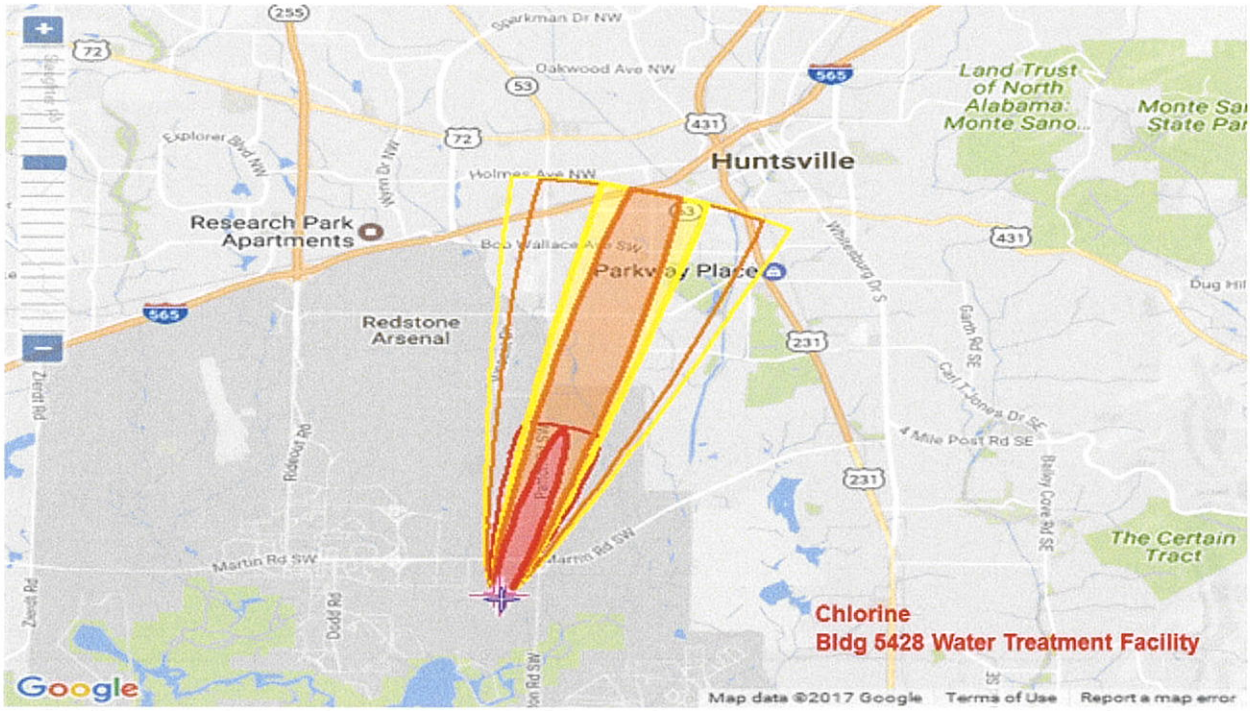
11. (U) Security Environment. The area surrounding Redstone Arsenal is a generally safe and secure area. Nearby civilian law enforcement agencies are supportive of the U.S military and cooperate on many levels. RSA's AT/FP efforts are assisted by the following law enforcement agencies: Marshall Space Flight Center, Huntsville Police Department, Madison Police Department, Madison County Sheriff's office, and the Federal Bureau of Investigation.

12. (FOUO) TICs/TIMs. There is a range of potential toxic chemical and toxic industrial substances/gases that could be employed in a low level terrorist attack. These attacks might occur in the form of a single generating device (i.e. a hydrogen cyanide device) or a large-scale deliberate release. Toxic Industrial Materials (TIMs) are readily available in larger volumes and less hazardous for terrorists to handle and deliver than Chem-Bio warfare agents.

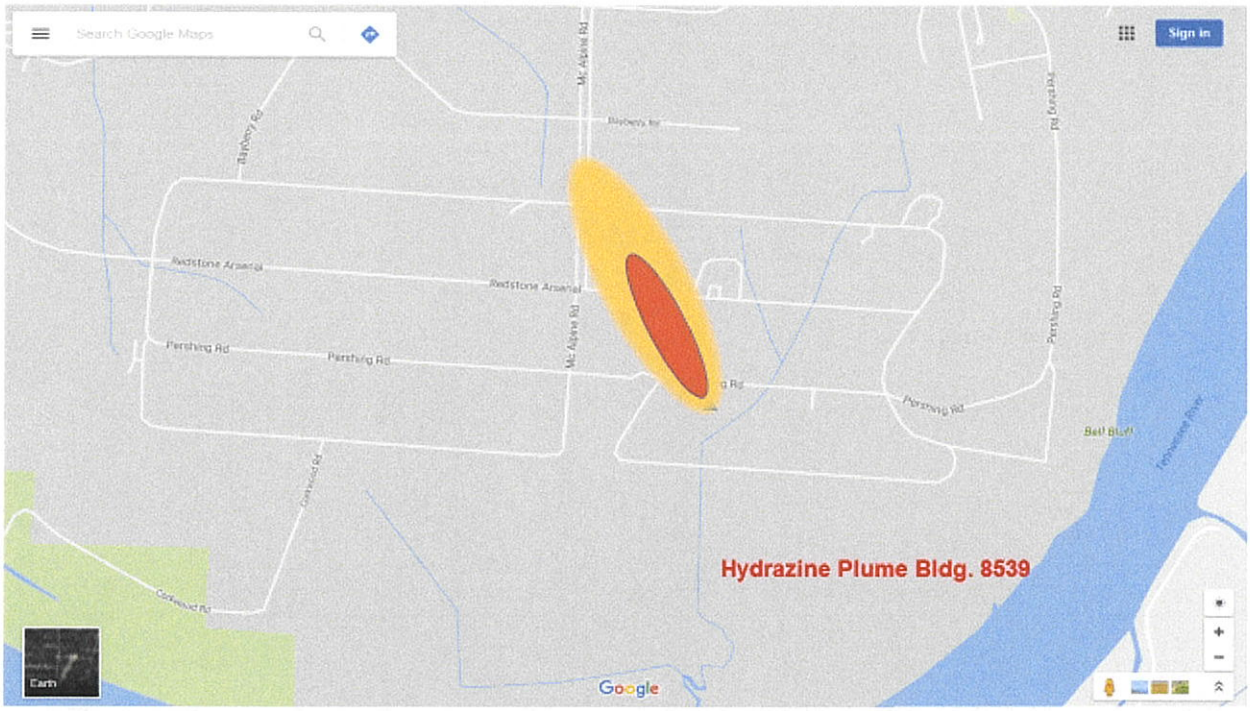
12.A. (U/FOUO) The TIC/TIM from an environmental sabotage may come in the form of commercial/ industrial sabotage or use of industrial chemicals to contaminate water supplies or create a large HAZMAT hazard. There are numerous industrial sites in Madison County that store large quantities of toxic substances-chlorine gas, ammonia, and hydrogen sulfide- that present an opportunity for sabotage. In addition, chlorine gas tanks employed for water treatment are located throughout the region. The bottom line is the threat of a TIC/TIM attack cannot be underestimated. In addition, these sites and substances, likewise, represent a potential for an accidental release.

12.B. (U/FOUO) Toxic Industrial Chemicals/Toxic Industrial Materials List:
This is the Redstone Arsenal Toxic Industrial Chemical/Toxic Industrial Material TICs/TIMs list that may affect the Redstone Arsenal Installation and or operations through contamination of the air. Five key TICs/TIMs were identified as very hazardous to the installation these were: Chlorine, Hydrazine, Nitric Acid, Nitrogen Dioxide, and Sulfuric Acid.

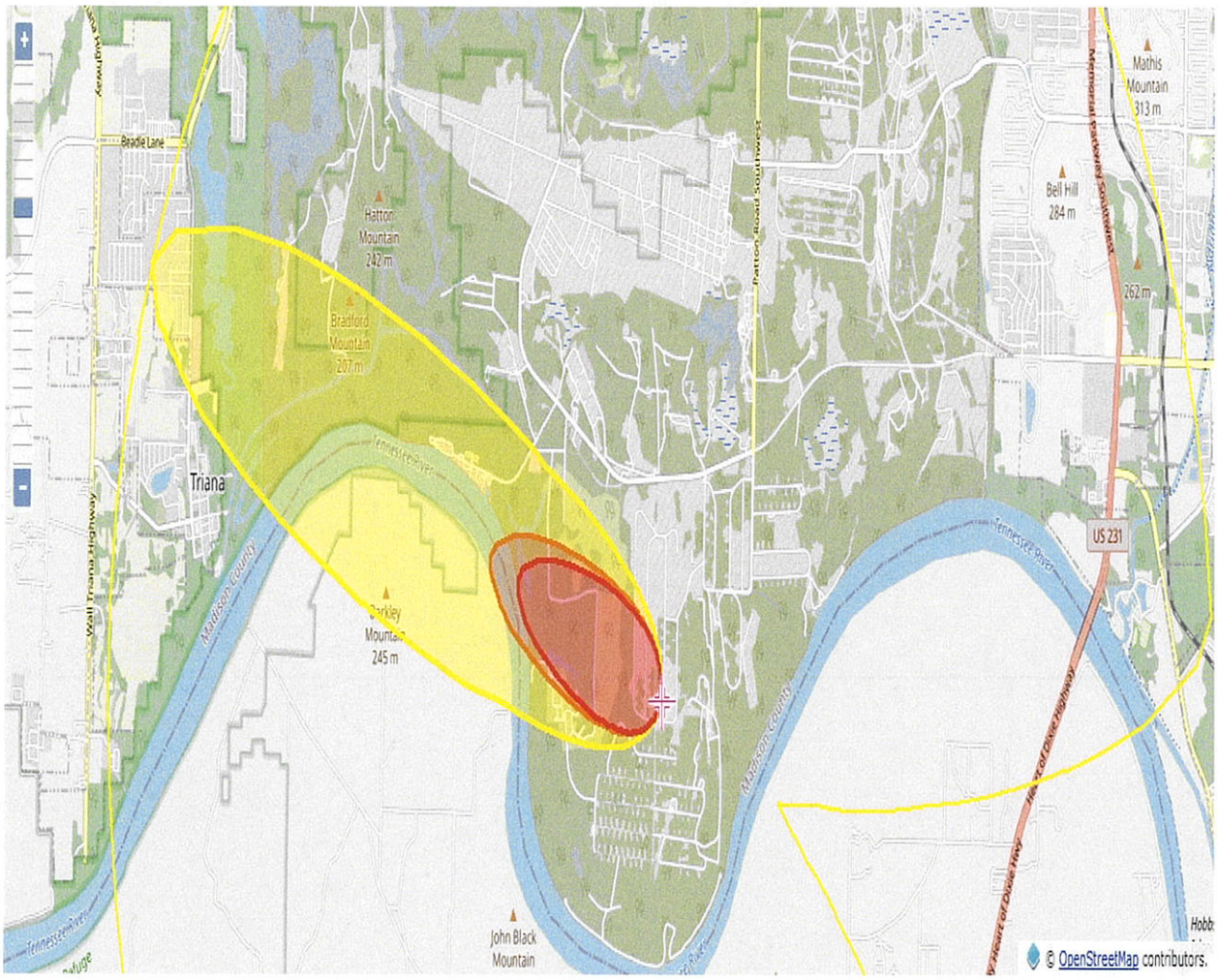
12.B.1. (U/FOUO) **Chlorine**-A colorless gas with a sweet odor. Toxic by inhalation and an irritant to skin, eyes and mucus membranes. Corrosive, heavier than air. Under prolonged exposure to fire or intense heat the containers may violently rupture. Used as an oxidizer in propellants. Contact with gas or liquefied gas may cause burns, severe injury and or frostbite. Toxic may be fatal if inhaled or absorbed through skin. Location of storage: **Bldg. 5428 Water Treatment Facility**, **6750 lbs.**



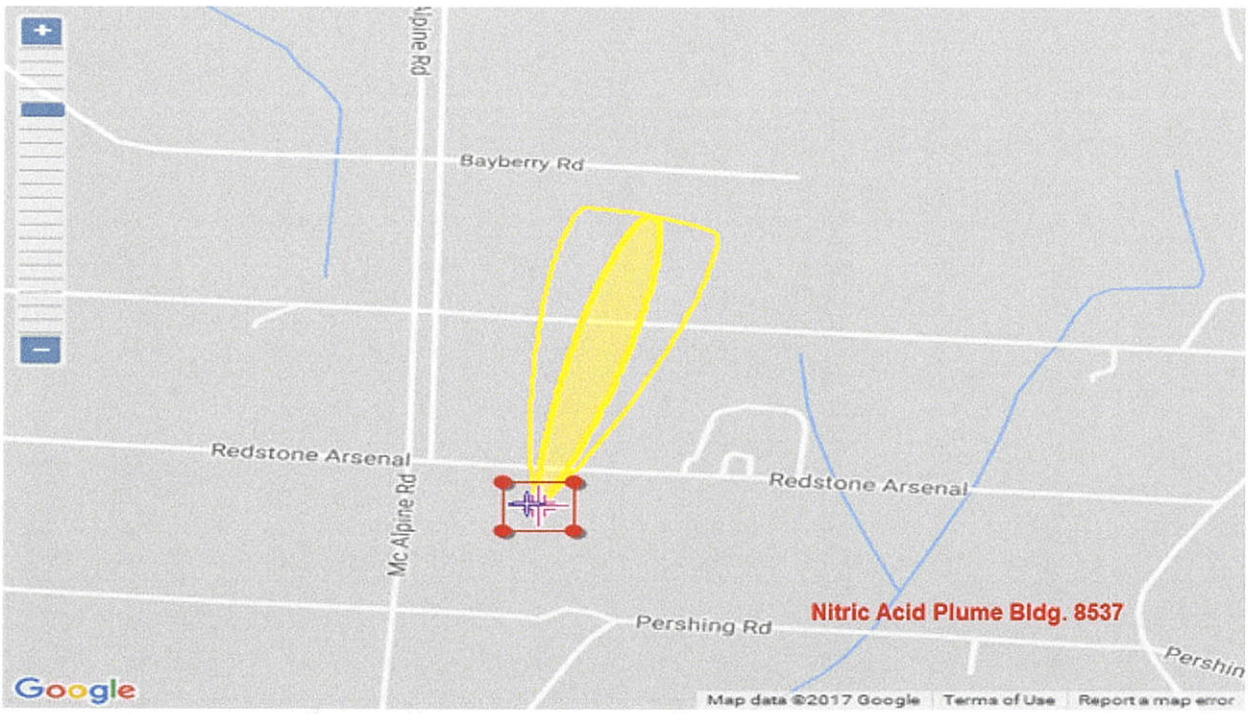
12.B.2. (U/FOUO) **Hydrazine**- Flammable/combustible material: may be ignited by heat, sparks or flames. Vapors may form explosive mixtures with air. Vapors may travel to source of ignition and flash back. Most vapors are heavier than air. They will spread along ground and collect in low or confined areas (sewers, basements, tanks). Vapor explosion hazard indoors, outdoors or in sewers. Location of storage: **Bldg. 8539 - 5364 gallons in liquid form.**



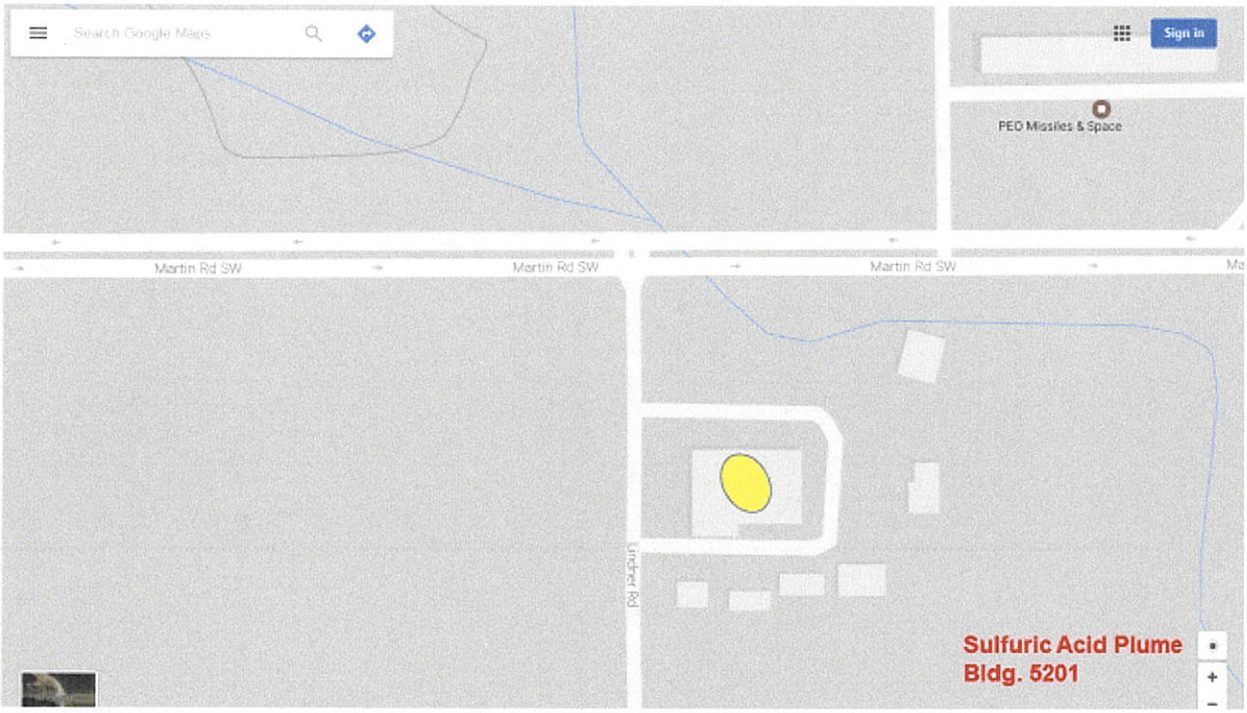
12.B.3. (U/FOUO) **Nitrogen Dioxide-** A reddish brown gas or yellowish-brown liquid when cooled or compressed. Shipped as a liquefied gas under own vapor pressure. Vapors are heavier than air and spread along the ground. Toxic by inhalation (vapor) and skin absorption. Noncombustible, but accelerates the burning of combustible materials. May be fatal if inhaled or adsorbed through skin. Fire will produce irritating, corrosive and or toxic gases. Cylinders exposed to fire may vent and release toxic and or corrosive gas through pressure relief devices. Location of storage: **Bldg. 8627 Amount: 3718 gal. = 44,233.80 lbs.**



12.B.4. (U/FOUO) **Nitric Acid**- A pale yellow to reddish brown liquid generating red-brown fumes and having a suffocating odor. Very toxic by inhalation. Prolonged exposure to low concentrations or short term exposure to high concentrations may result in adverse health effects. Substances will accelerate burning when involved in a fire. Containers may explode when heated. May react explosively with hydrocarbons (fuel). Location of storage: **Bldg.8537 Amount: 4594 gls. = 37,629.50 lbs.**



12.B.5. (U/FOUO) **Sulfuric Acid-** Sulfuric acid is a colorless oily liquid. It is soluble in water with release of heat. It is corrosive to metals and tissue. It will char wood and most other organic matter on contact, but is unlikely to cause a fire. Density 15 lb. / gal. Long term exposure to low concentrations or short term exposure to high concentrations can result in adverse health effects from inhalation. It is used in petroleum refining, in iron and steel production, and for many other uses. Sulfuric Acid is present at the facility in battery electrolyte and lead-acid batteries. The lead-acid batteries are industrial type batteries linked together. Location of storage: **Bldg.5201- 5772 lbs. of the electrolyte x .20 = 1154.4 lbs. (bulk batteries)**.



12.C. (U/FOUO) Chemical Weapons. Threat is based upon well-understood science, but weaponization has proven difficult. An incident of opportunity with the railway running near Redstone Arsenal would be of greater concern if HAZMAT cargo were attacked. Also of concern is the targeting of chemical industry facilities on or near the post. An attack at these sites has the potential to affect thousands of persons directly and to impact mobilization/deployment operations. An attack of this nature would most likely be initiated by a foreign (al Qa'ida or ISIS) terrorist cell. The combination of casualties produced and economic impact would fit their planning parameters.

12.D. (U/FOUO) Biological Weapons. We assess the likelihood of terrorists using biological weapons against Redstone Arsenal as a ***VERY LOW risk***. The most likely use of anthrax against the installation remains employment by a single perpetrator using mail as a means of dissemination.

12.E. (U/FOUO) Nuclear/Radiological Weapons. We assess the likelihood of a Radiological Dispersal Device (RDD) or dirty bomb, affecting the installation as ***LOW***. Use of a nuclear device against Redstone Arsenal is a ***VERY LOW risk***. For this class of weapons the threat is from the RDD, rather than from a nuclear weapon. Successful deployment of a radiological device will lack the destructive force of a nuclear bomb; it may however kill many in an urban setting and could conceivably render the area unlivable for months while posing cancer risks for decades. Initial casualties would likely be limited to the explosion itself. The effect of a dirty bomb is more likely calculated to gain recognition and make a statement while producing far more fear rather than casualties.

12.F. (U/FOUO) High-yield explosives are easy to acquire, but we assess the threat against Redstone Arsenal as a ***LOW risk***. Explosives range from military grade explosives (C4), mining explosives (dynamite), to home-made explosives such as ammonium nitrate fertilizer mixed with fuel oil (ANFO).

13. (U) Miscellaneous. This threat assessment covers Redstone Arsenal, Alabama and our area of responsibility. Redstone Arsenal is primarily a civilian base with over 38,000 civilians and only approximately 800 permanent party Soldiers. Redstone Arsenal is an integral member of the Huntsville and Madison County, Alabama community and has a great relationship with community leaders and business owners. RSA also has an outstanding working relationship with its emergency and disaster response mutual aid partners. These organizations participate in various installation level exercises and drills throughout the year.

14. (U) Points of Contact for Incident Reporting and Feedback. The following individuals/organizations have been assigned leads for providing specific data analysis supporting this assessment:

Agency	Name:	Contact info	Section(s)
DO (AT)	Dan Huber	(256) 842-2182	Design Basis Threat Terrorist Threat Extremists / Hate Bias Groups
DO (EM)	Tami Black	(256) 842-5453	Severe Weather Threat WMD/CBRN Threat
DO (PS)	Brian Reinwald	(256) 876-6815	Civil Disturbance Security Statement
CID	Richard Browning	(256) 876-9682	Criminal Threat Activity Local Gang Activity
RSA 902nd MI	(SA) Michael Gonzalez	(256) 876-8005	Foreign Intelligence Entity Threats
RNECC-R	Aaron Ford	(256) 842-6054	Cyber Threat
FAHC	Anthony Erskine	(256) 955-8888 ext 1125	Medical/Health/Safety
RSA Vet Services	SGT Kendall Long	(256) 842-7874 / (256) 955-8888 ext 1511	Food/Water Contamination Threat

15. (U) Prepared By: This assessment was compiled collaboratively by the Threat Working Group (TWG) and approved by the Garrison Commander. Any questions should be addressed to the RSA AT Program Manager, Daniel W. Huber at (256) 842-2182 or daniel.w.huber.civ@mail.mil for a coordinated working group response.

KELSEY A. SMITH
COL, AV
Commanding