[redacted] Unclassified

[redacted]

SF-0476-96
Copy 1 of 2A

Integrated Capabilities Assessment

of the

U.S. Army Medical Research Institute of Infectious Disease (U)

September 1996

THIS DOCUMENT IS FOR OFFICIAL USE ONLY.

Final Classification Determination Pending USAMRIID Review.

USAMRIID Control
01-RIID-7

[redacted] Unclassified

[redacted]

ARMY02-010530

unclassified

[redacted]

Integrated Capabilities Assessment

of the

U.S. Army Medical Research Institute of Infectious Disease

September 1996

[redacted] Unclassified [redacted]

[redacted]

Summary of the

Integrated Capabilities Assessment

of the

U.S. Army Medical Research Institute of Infectious Disease (U)

September 1996

[redacted]

Final Classification Determination Pending USAMRIID Review.

unclassified

[redacted]

(U) OVERVIEW

(U) An Integrated Capabilities Assessment was conducted at the US Army Medical Research Institute of Infectious Disease (USAMRIID) during the month of September 1996. The purpose of the assessment was to identify any vulnerabilities that could result in the loss or disruption of the USAMRIID functions, and to provide recommendations that would curtail the possibility of vulnerability. Although the team understood the necessity of an "open institute", the primary focus was to provide recommendations with regard to protecting USAMRIID, its people and functions.

(U) CONCLUSIONS AND MAJOR RECOMMENDATIONS

[redacted] Although some very good points are made throughout the assessment, there are a few issues that may require some additional attention. USAMRIID is at risk from a terrorist attack, especially with the growing role of biological weapons. It is believed that USAMRIID underestimates this risk. To safely operate in the new threat environment, USAMRIID must evolve to the next level of security.

"Open" does not have to mean defenseless.

[redacted] Major recommendations are as follows: (The details for each of these recommendations are provided in the following sections.)

- [redacted]

[redacted]

unclassified.

[redacted] unclassified [redacted]

(U) ASSESSMENT TEAM

(U) The assessment was conducted by an inter-agency team of engineers, analysts, and medical doctors with fourteen participants from the following organizations:

Argonne National Laboratory (ANL)
Armed Forces Radiobiology Research Institute (AFRRI)
U.S. Army Corps of Engineers, Omaha District (COE)
Industrial Analysis Support Office (IASO)
National Naval Medical Center, Infectious Disease Center
National Security Agency (NSA)
Defense Special Weapons Agency\Springfield Research Facility (DSWA\SRF)

(U) ASSESSMENT AREAS

(U) Most areas of USAMRIID were explored both functionally and physically. In addition, the Ft. Detrick Army Post was reviewed regarding the support and security that is provided but was not assessed. The buildings identified for the assessment included 1425, 1412, 1414, 1301, and Area B. The main building 1425 was the primary focus. A cursory review was conducted at the Area B, and only those relevant disciplines were applied to the remaining buildings. The following table lists the technical disciplines that were covered in the assessment of each of the buildings.

UNCLASSIFIED

Technical Discipline	1425	1412	1414	1301	Area B
Structural Survivability	X	X	X	X	X
Physical Security	X	X	X	X	X
Support Systems	X	X	X		
Fire Protection	X	X	X	X	X
Emergency Preparedness	X	X	X		
Operations	X	X			
Communications	X	X	X		
Network Assurance	X	X			
Industrial Base	X	X			

[redacted] unclassified [redacted]

(U) The technical disciplines that were applied in the assessment are defined as follows:

(U) **Structural Survivability**. The physical plant assessment focuses on the structures and physical protective features associated with the site and their capabilities to survive and support operations across the spectrum of environments and threats to which the site may be exposed. Items examined in the assessment typically include: the physical characteristics of the primary and supporting structures within the complex including the building plans (civil, structural, and architectural drawings); any geotechnical survey from the original construction and/or for any new construction in the near vicinity; critical element fragility and if available, the fragility of key supporting subsystems such as diesel generators, HVAC equipment, transformers, etc.

(U) **Security**. Security assessments investigate items relating to access control, penetration control, and other factors affecting a facility's physical security, operational integrity, and mission accomplishment. Items examined typically include: access control systems, such as card readers, surveillance cameras, and guards; perimeter control systems such as fences, sensors on fences, lighting, and guard posts; and procedures for day-to-day security and for dealing with security emergencies such as bomb threats, bombings, and terrorists activities.

(U) **Support Systems**. Support system assessments focus on the installation elements which support human life and the operation of mission equipment, i.e. life support systems, power generation and distribution systems, and environmental control systems. Life Support Systems include elements required to sustain human life, such as air revitalization equipment. Power generation and distribution systems include power sources, control equipment and equipment for the distribution of electrical power from the power sources to end-user loads. Several power sources may be employed to ensure a continuous supply of power through all potential operating environments. Environmental control systems include elements required for temperature and humidity control and typically comprise cooling, heating and heat dissipation elements. The information necessary to support the assessment will be derived through the examination of the electrical drawings, equipment (i.e. diesels, air conditioning, etc.), discussions with site personnel, and, as appropriate, data derived from manufacturers. Part of the assessment will focus on whether emergency operation subsystems can support the required endurance requirements.

(U) **Fire Protection**. Fire Protection focuses on the site's existing protective features for accidents or incidents, such as fires, equipment available for responding to accidents, and training and procedures of personnel for supporting such responses. Items examined in the assessment typically include: sensors for smoke/fire detection, control and alarm panels, organic fire fighting equipment, the ventilation system design for smoke removal, and the interface with external firefighters; personnel training for dealing with disasters such as fires, tests, and as appropriate exercises; materials

that would increase the risk of an accident or fire, such as concentrations of flammable materials that produce an increased fire load; and the tools that the staff has to handle an incident or contain it until outside help is available.

(U) **Operations**. The primary focus of the operations assessment is the the procedures or process followed in performing the critical function at the primary site and at back-up locations including critical internal and external interfaces, personnel required to support the process, and how the critical function degrades when key components are damaged or disrupted.

(U) **Communications**. Communications assessments focus on the ability to receive and transfer information related to the facility's mission or operations. The assessment typically focuses on internal and external communications systems.

(U) **Network Analysis**. Although netowrk analysis is normally incorporated in the communications assessment it is separated to focus on internal and external communications/computer networks which are necessary to support process/operations and their potential vulnerability to electronic exploitation. Typical areas for this assessment include: internal network topology, system administration, locations of file servers, terminals, network software, and security; external network topology, interfaces, access controls, fire breaks, security; procedures for granting access, establishing passwords, identifying unauthorized intrusion, and for determining files, programs or control has been tampered with.

(U) **Industrial Analysis**. The primary focus of the an industrial analysis is to ensure the availability of industrial resources necessary to support a vital capability. The items typically examined in the assessment include: capabilities (skills, processes, facilities and technology) utilized in production, financial (assets, debts, past and present sales) and economic (current market, potential customer base). All of this information is collected and integrated into one analysis. The information is obtained from on site visits to the company, the DoD customer, the Defense Contract Audit Agency (DCAA), on-line financial data sources.

unclassified

(U) **THREAT**

(U) The assessment was conducted based on a defined threat. The broad spectrum of threat issues that were considered can be divided into two types of assaults, internal and external. Accidents, criminal activity, and sabotage/espionage are considered to be internal assaults. Terrorism, info-warfare, and natural disasters are categorized as external assaults. Great concern for terrorism is warranted particulary armed intruders and vehicles carrying explosives. Unfortunately, terrorism is becoming a problem that cannot be ignored.

(U) The table below provides examples of the types of threat:

UNCLASSIFIED

THREAT	TYPICAL ELEMENTS
Internal Assaults	
Accidents	Fire, smoke, HAZMAT contamination, structure failure
Criminal Activity	Arson, personal assault, vandalism
Sabotage/Espionage	Tampering, arson, data manipulation, data theft
External Assaults	
Terrorism	Car/truck bombs, RPGs, incendiaries/duress
Infowarfare	Viruses, Trojan horses, data alteration
Civil Unrest	Protest, rioting, looting
Natural Disaster\ Technical Failure	Tornadoes, hurricanes, floods, aircraft crashes
Conventional	Aircraft bombs & missiles, surface to surface weapons

(U) An example of terrorism that relates specifically to USAMRIID is the animal rights activists. There are currently over 7000 activist groups in the United States. The Animal Liberation Front (ALF) is recognized as one of the most violent of the groups. The FBI classifies ALF activists as terrorists. ALF originated in the UK and currently commits approximately 100 attacks per month in the UK and the attacks are becoming more and more violent. The trend has been for the US activists to follow the examples set in the UK. The People for the Ethical Treatment of Animals (PETA) is highly suspected to be the political arm for ALF. It is common practice for PETA to alert the media in the instance of an ALF attack, and also, PETA has been known to pay ALF legal expenses. PETA

has an operating budget of over $8 million. Animal researchers have been identified as prime targets for animal activists. Most attacks are aimed at preventing a major breakthrough in order to cause the institute the greatest loss possible. Institutes are targeted by information gathered regarding grants, through FOIA requests, researching medical journals, INTERNET, and other forms of publicity. (This information was obtained directly from the American for Medical Progress Organization and also from several WEB sites on the INTERNET.)

(U) There are some issues that should be considered in reference to defining the threat. Most at USAMRIID are certain that the amounts of agent used openly at any given time are so small that there is minimal potential threat to the community in the event that an incident occurs. However, the wrong perception of an agent release by the public could actually be worse than the results of the incident. Consequently, if a release did occur, there is the potential for casualties which would not only be a devastating event, but would also draw national attention.

(U) Another issue that should be seriously considered is the consequences should agents be stolen. Agents that end up in the possession of either domestic terrorists or foreign terrorist states could easily become biological warfare capable. The results of such an incident could not only cause national level disaster but potential international havoc.

(U) In addition to the threat, issues specific to the uniqueness of USAMRIID were also considered. USAMRIID is the primary source for advice and sample analysis in the event of a national incident. Both the people and laboratories are vital to the prevention and treatment against biological attack. The BL4 laboratories are one of only two in the country. The staff at USAMRIID should be considered national technical assets.

[redacted] unclassified [redacted]

[redacted]

(U) **ASSESSMENT**

(U) The assessment is described below:

(U) **RISK Analysis**

(U) A number of potential risk situations perceived by personnel at USAMRIID are outlined below. The risks are divided into two categories, medium to high probability, and low probability. It should not be forgotten that situations considered low probability could result in a devastating outcome. The assessment team attempted to determine the likelihood of the these situations occurring.

[redacted] Situations perceived by USAMRIID to be of high risk included:

- [redacted] Maintaining the reputation of USAMRIID as an open research institute is one issue of high concern. *In order to maintain an "open institute", security issues are placed at a lower priority if there is potential that added security will jeopardize that reputation. Also, the publicity associated with sharing breakthroughs in research may increase the potential of attacks by animal rights activists.*

- [redacted] Many of those at USAMRIID believe that animal rights activists are the highest potential threat. *This is a possible risk to USAMRIID and the probability seems to be increasing. However, currently the animal rights activists are being challenged by the Aids research activists. Many support both groups - you can't have it both ways.*

- [redacted] Open post has reduced the overall security at USAMRIID. *This is a very true statement, however a closed post will not stop those who really want in, such as some sort of terrorist.*

[redacted] Low risk situations perceived by USAMRIID include the following:

- [redacted] The potential of release of animals into the community. *Either infected or not the public response could be devastating. For this to happen, however, it would most likely be an animal activist "mole" or an innocent act by an insider who desires a new pet.*

- [redacted] Thefts of agents by insiders or outsiders. *Although not very probable, it is believed that a theft would most likely occur from an insider simple from accessibility.*

~~SECRET~~

[redacted] unclassified [redacted]

- (U) Actions by disgruntled employees could include anything from "negative press" to hostile behavior. *This is considered an unlikely situation based on the maturity of the staff that is necessary to function at USAMRIID.*

- (U) There appears to be little concern towrds terrorist attacks. However, the PMO has stated the threat level is medium to high due to potential terrorism. *This could be more probable than viewed by the USAMRIID staff. Terrorism is growing and USAMRIID does have a critical role in a national crisis.*

- (U) The release of agents into the community through accident or other causes does not seem to be considered very probable. Although if it were to happen, the results would be catastrophic.

(U) In general, personnel do not feel threatened and "USAMRIID has things under control."

(U) The team also identified situations that could put USAMRIID at risk. They are as follows:

- (U) The Oklahoma bombing is only one example of a terrorist attack in which the only objective was total destruction.

- (U) As mentioned above the theft of agents either from insiders or intruders would have devastating repercussions. With the growing interest in biological weapons the potential for this could increase.

- (U) The event of technological failures such as power failure or damage caused by fire could not only result in a disruption in day to day activities but could also result in the loss of research.

- (U) With the high publicity of several Sr. scientists, a duress/kidnap situation has probability. A person whose ambition is to either access the facility or to steal agents could use this method to quietly accomplish the intentions.

(U) **Structural Survivability**

(U) All of the buildings at USAMRIID are of standard frame construction, built to conform standard design practice not designed to resist attack. In the event of any type of blast, large or small, the buildings will not provide protection from the effects. The fact that most labs are not located on exterior walls will help to reduce damage to critical areas. The two mechanical floors in building

1425 and the single mechanical floor in 1412 will add protection from a penetration through the roof. (This could include a helicopter crash.)

(U) In addition to the building construction, the doors and windows are also not hardened. An example of improving doors would be to change from opening into the facility to opening out. Lamination on windows help protect against glass fragments.

(U) Vehicles have become the desired method of delivery by terrorists. The fact that vehicles can currently park in very close proximity to the buildings would increase the damage effects in the event of a blast.

(U) **Physical Security**

(U) Assessment of USAMRIID's physical security examined three primary areas: vehicle access and control, intrusion deterrence and detection, and personnel access and control. The following findings and primary recommendations resulted from the three week examination.

(U) The security office and guard force are knowledgeable, well trained, and professional. It is recommended that the force be designated as security "police"rather than guards to give them arrest authority and to open the pool of applicants for the positions. It should be emphasized that the manning of the guard force should be by force personnel, not military helpers. Use of 'helpers' only reinforces the need to fill the empty billets and add more, a requirement if the security recommendations are embraced. The security force suffers from an apparent lack of authority from the perspective of enforcement of security policies - non-compliance, particularly when blatant, should be dealt with properly. There are an excellent badging system and an internal intrusion detection system in place - minor improvements here.

(U) Vulnerabilities of primary concern include at the head of the list, the dispensary. This should be separated from USAMRIID as soon as possible - sooner if practicable. It presents one of the biggest weaknesses with regard to unauthorized personnel access. Vehicle control is next to non-existent - primarily due to the open post, but also with regard to the 90's DoD exclusion zone standards being applied. Likewise, there is easy access to the grounds, within briefcase threat zones, by unauthorized personnel. To abate this access control problem by both vehicles and people, parking lots must be relocated, roads adjustments made per the briefing, vehicle access control point established, and a fence constructed per the briefing surrounding 1425 and 1412 with a designated visitor entrance. Fence exclusion zone is 110 feet minimum; road access exclusion is 300 feet minimum. This is the singularly most important modification to be made once the dispensary is relocated.

(U) A duress procedure should be implemented at a minimum for critical personnel (Vault access people, commander, Sr. Scientists, security force, etc.) To preclude access by hostile individuals or groups. Duress is a possible occurrence that few organizations recognize. NACI checks should be done on anyone who works inside the buildings unescorted. This is especially true for contractors and students who are not employees but who would work in the area for an extended period of time. If they aren't there long enough for a NACI, they must be escorted. Ward 200 Protocol volunteers should have their baggage and person searched - you've all ready had one knife incident and not searching is begging for trouble.

(U) Security awareness must be reinforced on a regular basis - not scare tactics but legitimate, responsible actions by employees to help preclude improper access and protocol. Access to facilities, especially critical components like those found in the Penthouse, must be controlled and limited. Focus on limiting and controlling access of people and vehicles is where the most is gained toward mitigating your risk.

(U) **Support Systems**

(U) A detailed description of the support systems is attached.

(U) **Fire Protection**

(U) USAMRIID has a well designed fire protection plan. The post fire department is well trained and equipped for handling situations with USAMRIID. Close relationships exist between USAMRIID and the fire department with information exchange and familiarity with the Institute. The central and remote monitoring fire alarm system aids in the rapid response in the event of a fire. The Integrated door control system provides for quick exit of the staff.

(U) Fire is the main threat to facility and life safety. Fire and life safety training should be conducted regularly as an integral of any facility safety program. USAMRIID has a good basic fire protection and containment program in place. However, as is the case with most facilities, there are program deficiencies and omissions. These are not always obvious to facility personnel. Periodic internal and external review are critical in maintaining an effective facility safety program.

(U) The following are a few things that could be done to either prevent or improve the protection of the facility and staff in the event of fire. The critical areas, specifically laboratories do not have fire suppression systems. This is do mostly to the age of the buildings. However, either sprinkler

[redacted]

systems or halon systems should be installed. Keep in mind sprinkler systems will also require modifications to the drainage process.

(U) There are an insufficient number of standpipe locations. The farther water has to travel decreases water pressure which could also be reduced to due current usage on the Post. These systems cannot be supplemented by the fire department.

(U) The Post fire department are the only ones with authorization to enter labs in the event of an emergency. There should be an internal response team given the short staff and extended commitments of the fire department.

(U) There is no formal emergency training for personnel including CPR, and the use of fire extinguishers. Even though it is not desired for personnel to use the extinguishers, in an emergency it will be human nature to attempt.

(U) Fire drills are not conducted on a regular basis and few of the escape routes are marked. In a military installation, personnel tends to be more transient, therefore, there should be some assurance that personnel are prepared for an emergency. Escape routes are especially necessary for visitors.

(U) **Emergency Preparedness**

(U) Both USAMRIID and the Post have well organized and structured Emergency Preparedness plans to address most emergency situations at USAMRIID. The Post appears to provide excellent support when necessary, however USAMRIID needs to keep close watch on the plans associated with the Fort Ritchie closure.

(U) There are a few things that can be done to improve the plans in the event of a catastrophic incident. The Public Affairs Office should be included in the regulations to clarify appropriate actions in the event of catastrophic event.

(U) The plans also don't address recovery procedures. To put the operation back on line as soon as possible plans should be defined.

(U) Procedures should be developed and disseminated in the event of complete loss of power in the BL3 and BL4 labs.

[redacted]

[redacted]

(U) The limitation of three radio communication channels could impair actions in an emergency situation. The acquisition of additional radio frequencies should be considered and/or develop priority of the use of the system.

(U) Helicopters accessing the adjacent pad fly over USAMRIID buildings and accidents do happen. The roof is not survivable to a helicopter crash and there are critical support systems located on the roof. It should be a reasonable request for the helicopters to use a different flight path.

(U) **Operations**

(U) The Operations assessment includes sort of a catch all for day-to-day activities and interfaces among personnel. Is a common problem to have simple miscommunications or innocent misunderstandings among staff that can potentially add to the risk of the facility. The main issue discovered during the assessment at USAMRIID was the fact the biosafety designations of containment labs vary among the staff. The maintenance personnel responsible for setting up the labs had one list, the safety office had a second list, and the security office had yet a third list. All three lists differed with the designations. This may or may not cause problems, however, it should be a fairly simple thing to resolve.

(U) Although the bio-safety procedures were not reviewed, the team did pursue inventory procedures and the two-man rule in the lab. The inventory is maintained and kept up to date, however, it is stored in one location. In the event of a fire or other damaging event, the inventory could be lost. The team was interested in the two-man rule for two reasons, 1) safety of those working in the lab, and 2) potential theft of agents. USAMRIID has posed very good arguments as to why the two-man rule really does not provide any benefit in comparison to the resources that would be drained if the rule were enforced.

(U) It is recommended that USAMRIID and the CDC formalize agreements to aid each other in the event one of the facilities experiences a disruption in operations.

(U) **Communications**

(U) During a crisis situation, a disruption in communications would impede operations. It is recommended that USAMRIID review the plans for providing alternate communication if the need should arise. Also, the purchase of an IMARSAT SATCOM STU II terminal should be considered along with cellular phones for key members of the staff.

[redacted]

unclassified

[redacted]

[redacted]

[redacted]

unclassified

(U) **Information & Network Assurance**

(U) The USAMRIID networks are not protected from unauthorized access. The National Security Agency will be conducting a penetration test. These results will determine exactly how vulnerable the USAMRIID network is.

(U) **Industrial Base**

(U) Over thirty items were identified as necessary to support BL4 laboratory operators. Preliminary evaluation is that all items are off-the-shelf and commercially available. The remaining issues are the acceptable delivery times and long-term viability of major suppliers.

[redacted]

(U) SUPPORT SYSTEMS DETAILED DESCRIPTION

(U) Strengths in the system:

1) (U) Multiple, independent electrical power feeds provide dual sources of normal municipal power and an emergency power supply for critical loads in buildings 1425 and 1412 during non-catastrophic utility power system mechanical failures and are-wide outages.

2) (U) Most critical mechanical support utilities have adequate system redundancy and have reasonable survivability relative to the building itself.

3) (U) Electrical power system switching from normal municipal sources, diesel generator auto-start, and emergency power system operation at full critical loads for several hours is tested once each month.

(U) Potential Problem Areas Summary:

1) [redacted]

2) [redacted]

3) [redacted]

4) [redacted]

5) [redacted]

[redacted]

[redacted]

(U) Detailed Description of Potential Problem Areas:

1) [redacted]

- [redacted]

[redacted]

(U) Recommendations:

[redacted] Shorter term: Increase security measures to prevent unauthorized vehicle access to the driveway and loading dock areas around building 1425's diesel generators and substation #3.

[redacted]

[redacted]

[redacted]

2) [redacted]

3) [redacted]

[redacted]

[redacted]

4) [redacted]

(U) Recommendations:

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

5) [redacted]

[redacted]

1) [redacted]

2) [redacted]

~~SECRET~~

[redacted]

[redacted]

Executive Briefing of the

Integrated Capabilities Assessment

of the

U.S. Army Medical Research Institute of Infectious Disease (U)

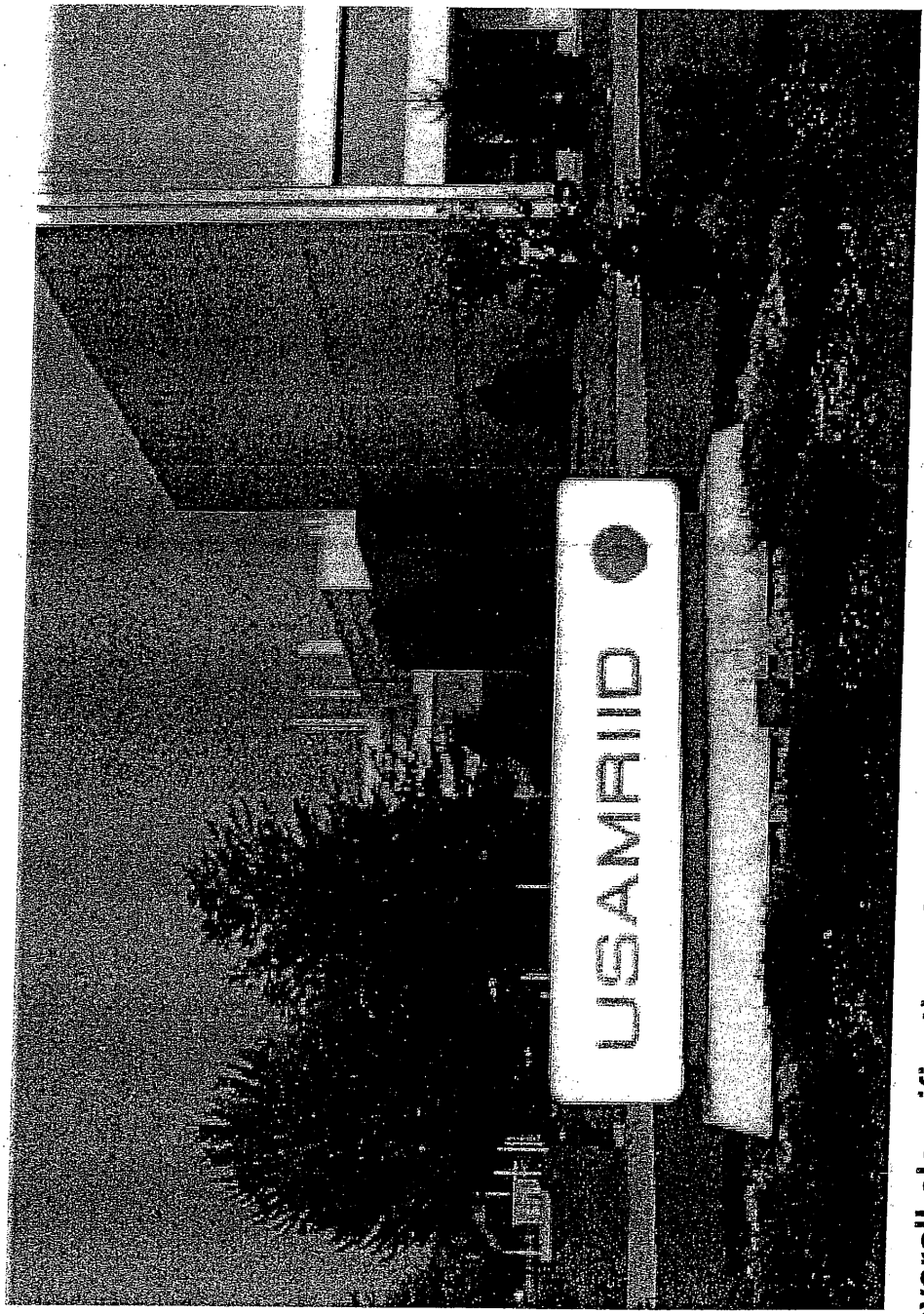
September 1996

THIS DOCUMENT IS FOR OFFICIAL USE ONLY.

Final Classification Determination Pending USAMRIID review.

[redacted]

[redacted]



The overall classification of this briefing is [redacted]

[redacted]

ARMY02-010553

INTEGRATED VULNERABILITY ASSESSMENT

OF THE

U.S. ARMY MEDICAL RESEARCH INSTITUTE

OF

INFECTIOUS DISEASES (U)

September 1996

The overall classification of this briefing is [redacted]

[redacted]

[redacted] SMAMRIIDBB

ARMY02-010555

Agenda

- Objectives
- Threats
- Assessment
- Conclusions
- Recommendations
- Summary

[redacted] SMAMRIID

ARMY02-010556

USAMRIID Assessment

- Objective was to accomplish a system vulnerability assessment
- Post functions which supply critical support services to USAMRIID were reviewed but not assessed
- While we understood the "open institute" concern, our focus is on protecting USAMRIID, its people and its functions

[redacted]

SMAMRIID

ARMY02-010557

Team Composition

- Argonne National Laboratory
- Armed Forces Radiobiological Research Institute
- Industrial Analysis Support Office
- National Naval Medical Center
- National Security Agency
- U.S. Army Corps of Engineers, Omaha District
- Defense Special Weapons Agency

Sixteen Experts Participated

[redacted]
SMAMRIID

ARMY02-010558

Elements Assessed

Assessment Area	1425	1412	1414	1301	FARM
Structural Survivability	X	X	X	X	X
Physical Security	X	X	X	X	X
Support Systems	X	X	X		
Fire Protection	X	X	X	X	X
Emergency Preparedness	X	X			
Operations	X	X			
Communications	X	X	X		
Network Analysis	X	X			
Industrial Base	X	X			

[redacted]

SMAMRIID

ARMY02-010559

Threat

Threat	Typical Elements
Internal Assaults	
Accidents Criminal Activity Sabotage/Espionage	Fire, smoke, HAZMAT contamination, structural failure Arson, personal assault, vandalism Tampering, arson, letter/satchel bombs/data/manipulation, theft
External Assaults	
Terrorism Infowarfare Civil Unrest Natural Disasters/ Technical Failure Conventional WMD	Car/truck bombs, RPGs, incendiaries/duress Viruses, Trojan horses, data alteration Rioting, looting, widespread arson Tornadoes, hurricanes, floods, earthquakes, dam bursts, aircraft crashes Aircraft bombs & missiles, surface-to-surface weapons Nuclear, chemical and biological

SMAMRIID

Animal Activists
(Americans for Medical Progress, et al)

- Over 7000 activist groups
  - 100 attacks a month in UK (increasing violence)
  - 80 attacks a year in the U.S.
- PETA and ALF major players
  - $8m budget
  - ALF is enforcement arm for PETA (per FBI)
- Prime targets are animal researchers
- Over 75 attacks in U.S. aimed at research labs
  - Aimed at preventing scientific breakthroughs
- Range of activities include arson, bombings, assassination, release of infected animals and vandalism
  - Many attacks on nights & weekends
- Sources include grants, FOIA requests, medical journals, Internet, etc.

Trend is toward more attacks and increased violence

[redacted]

SMAMRIID

ARMY02-010561

Drug May Cure Ebola Fever

Mouse study shows promise

By Laurie Garrett
STAFF WRITER

Antwerp, Belgium — **U.S. Army medical researchers have found a drug that may be useful in treating Ebola hemorrhagic fever** and may turn out to be a cure for the disease, which has proven fatal in 60 to 90 percent of all cases.

Test tube studies of infected monkey cells and use of the intravenous drug in infected mice have proven 100 percent effective in clearing the virus.

"Our final conclusion is it looks like a therapeutic intervention that can be done," [redacted] of the U[redacted] States Army Medical Research In[redacted] on Infectious Diseases (USAMRIID) told scientists gathered here for the International Colloquium on Ebola Virus Research.

Dr. Karl Johnson, who headed international efforts to stop the first Ebola epidemic in Zaire in 1976, reacted to Huggins' announcement with excitement.

"It really does look as though there may be a drug, finally," Johnson said.

Dr. C. J. Peters, who heads the Centers for Disease Control and Prevention's Special Pathogens Laboratory, greeted the drug announcement with obvious relief. He said there was a desperate need for something that scientists, like himself, who work with Ebola, could take if they accidentally became infected in the laboratory. Clearly, if the USAMRIID drug proves effective in humans, it will be a boon for all future victims of the virus.

But observers warned that it is a long way from mouse studies to clinical trials in human patients, and manufacture of the drug has proven tedious and costly.

"I think with luck we can get this into monkey trials within six months," Huggins said in an interview. "Dollars clearly are going to drive the speed that we can go forward on this thing."

Because of Department of Defense cutbacks and lack of interest from drug companies, Huggins said, his lab is far short of the necessary funds to get the drug into clinical development.

The drug, which is called Cac3-Abo, is one of the hundreds that USAMRIID received from drug companies when it put out queries asking for otherwise useless compounds the pharmaceutical manufacturers had on their shelves — chemicals known to block another chemical called adenosylhomocysteine hydrolase. That chemical is essential to the Ebola virus' reproductive cycle.

Research on the compounds moved at a plodding pace for two years, until **USAMRIID's Dr. Michael Bray** figured out a way to make mice develop Ebola disease. Once that was accomplished, the mice became a quick way to screen drugs for their efficacy against Ebola.

Special Considerations

- People and labs are vital to biological defense
  - First stop for advice, data and analysis
  - Development of vaccines, treatments and diagnostic measures for BW
- Many of scientific staff are national assets
- Release (or perception of release) of agents could impact community and draw national attention
- Serious downside if agent stolen
  - Sale to terrorist state
  - BW capability for domestic terrorists

USAMRIID is unique

[redacted]

SMAMRIID

ARMY02-010563

USAMRIID Assessment

- Risk
- Structural Survivability
- Physical Security
- Support Systems
- Fire Protection
- Emergency Preparedness
- Operations
- Communications
- Information & Network Assurance
- Industrial Base Analysis

[redacted]
SMAMRIID

ARMY02-010564

Risks Perceived by USAMRIID

Medium to High

- Any action that jeopardizes USAMRIID's reputation as an open research institute
- Open Post has reduced overall security
- Protests or attacks by animal activists

Low

- Release of infected animals
- Theft of agents by insiders or outsiders
- Release of agents through accidents or other causes
- Actions by disgruntled employees
- Attack by terrorist groups (PM differs)

In general, personnel do not feel threatened and "USAMRIID has things under control"

[redacted]

SMAMRIID

ARMY02-010565

Risks Perceived by Team

- Oklahoma City Situation
  - Destruction of the facility is the objective
- Agents stolen or removed from laboratories
  - Insiders or intruders
- Technological Failures
  - Fire, electrical failure, computer failure, etc.
- Disgruntled Employee
  - Revenge on individual, office or institution
- Kidnap/duress situations
  - Quiet entry to highly sensitive locations

[redacted]

SMAMRIID

ARMY02-010566

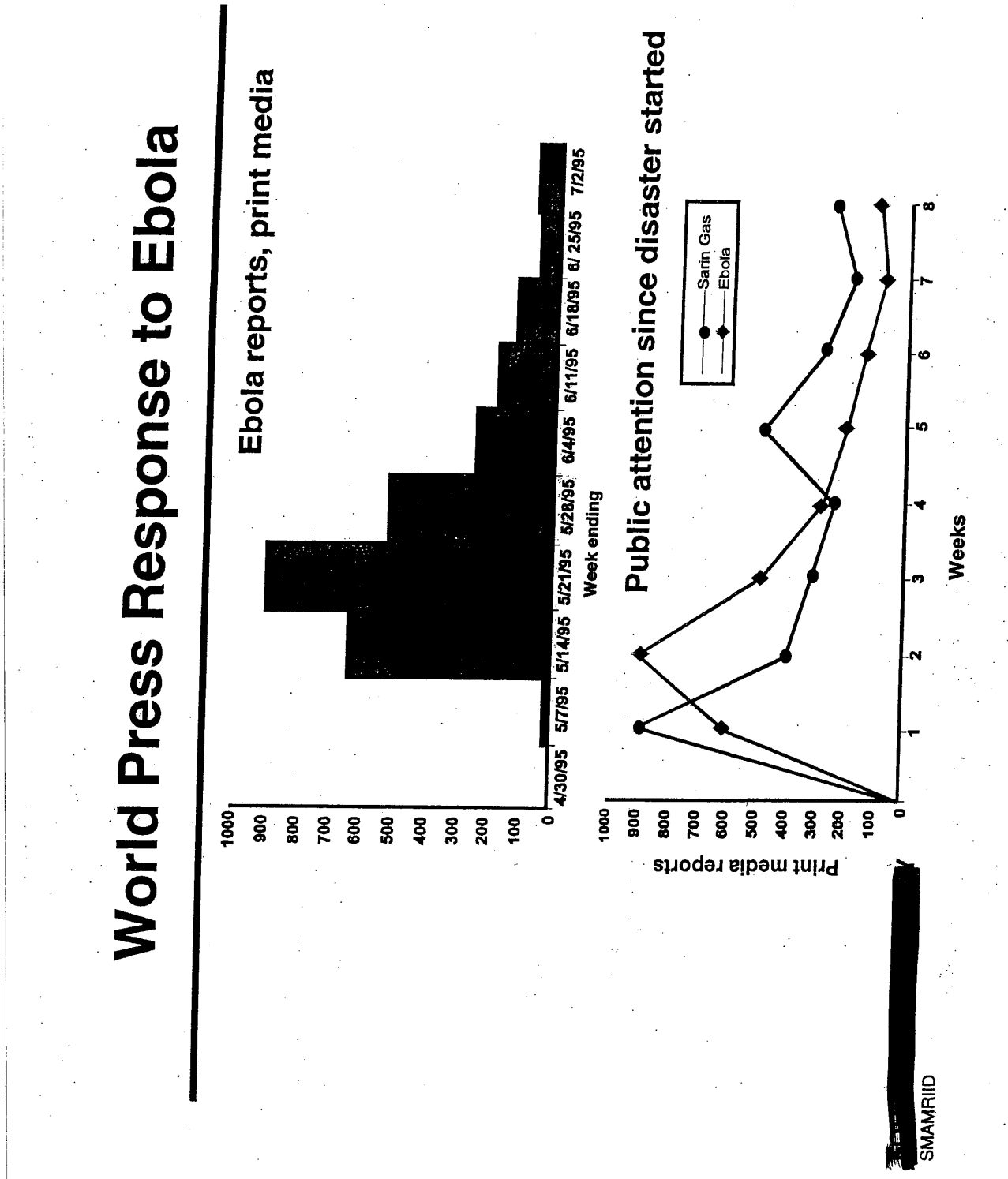
Other Risk Considerations

- USAMRIID's role in national crisis response not advertised
- Ft. Detrick's location provides a degree of protection
- Animal activists know USAMRIID does research on animals
- Anything connected with Ebola draws world-wide media attention
- Ft. Detrick is likely to remain an open Post

[redacted]

SMAMRIID

ARMY02-010567



ARMY02-010568

Structural Analysis

- All USAMRIID buildings are of standard frame construction
  - Not hardened for blast effects
  - Most labs do not have exterior windows
  - Most labs are not on exterior walls
- Unhardened doors and ground level windows will not deter a determined intruder
- Vehicles can be parked next to the walls of both buildings

Buildings do not provide protection from blast effects

[redacted] SMAMRIID

ARMY02-010569

Physical Security

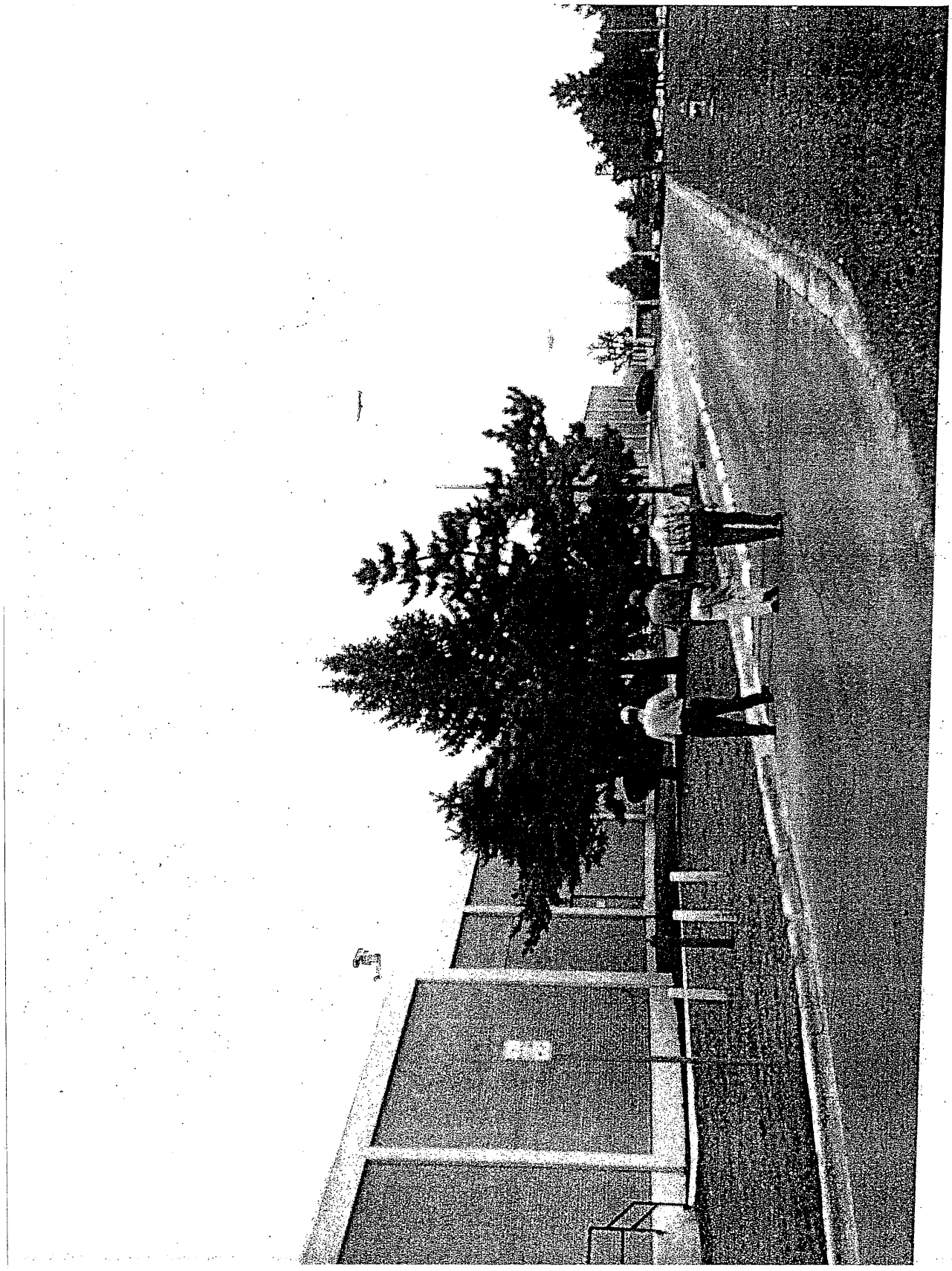
- CoE and DSWA team accomplished review
- Recommendations divided into three categories
  - Vehicles issues
  - Intrusion prevention
  - People issues

Security force knowledgeable, well trained and professional--PMO provides good support

[redacted]

SMAMRIID

ARMY02-010570



ARMY02-010571

Security-Vehicles

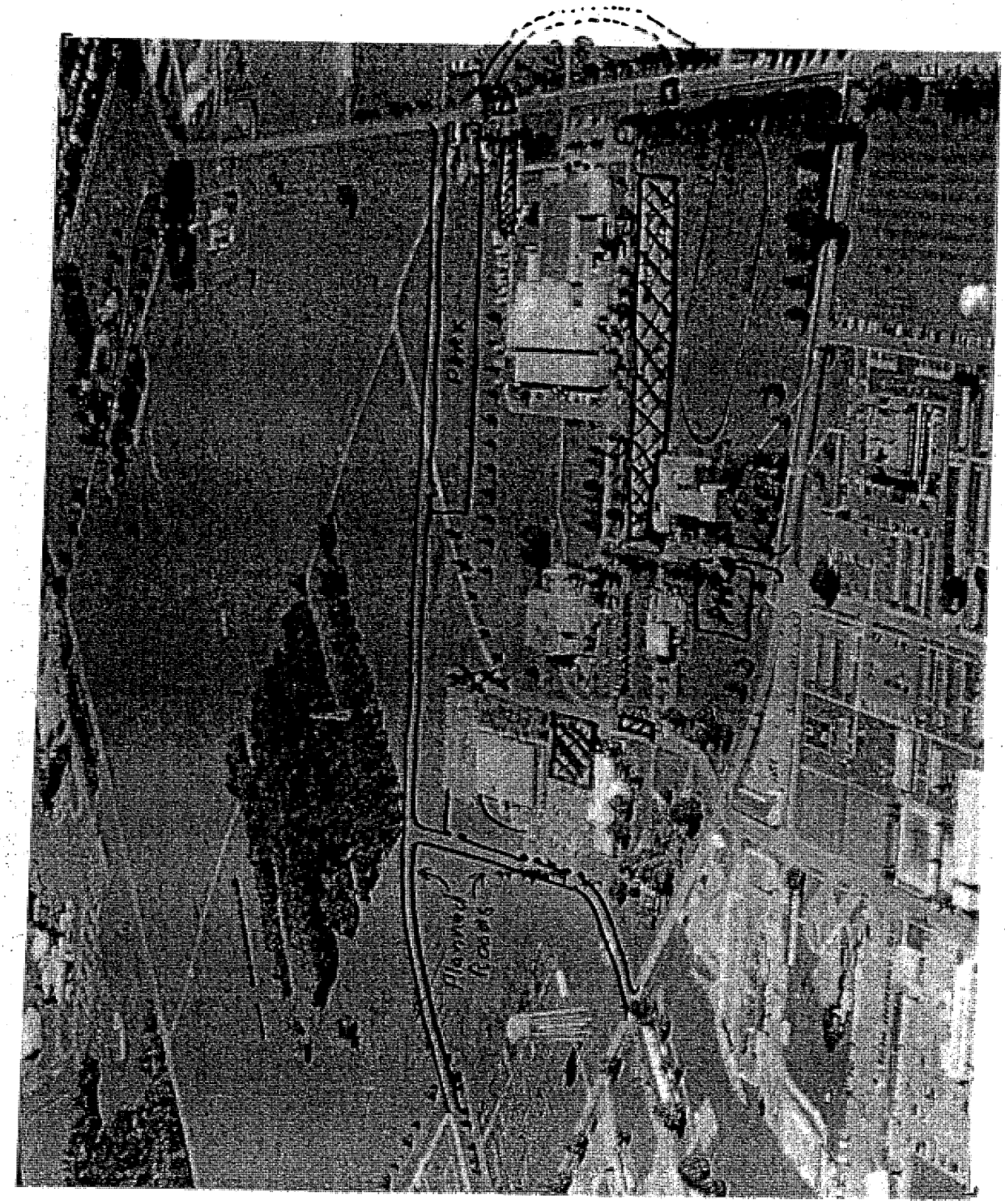
- Place bollards or concrete planters at entrances
- Use a swingarm gate to restrict rear access road
  - Alternative is "no parking" fire lane
- Except for animals, channel all deliveries to post receiving
  - U.S. Govt vehicles only in loading docks
- Restrict vehicles within 320 ft of Bldgs 1425 & 1412

Stationary vehicle bomb protection measures

[redacted]

SMAMRIID

ARMY02-010572



ARMY02-010573

[redacted]

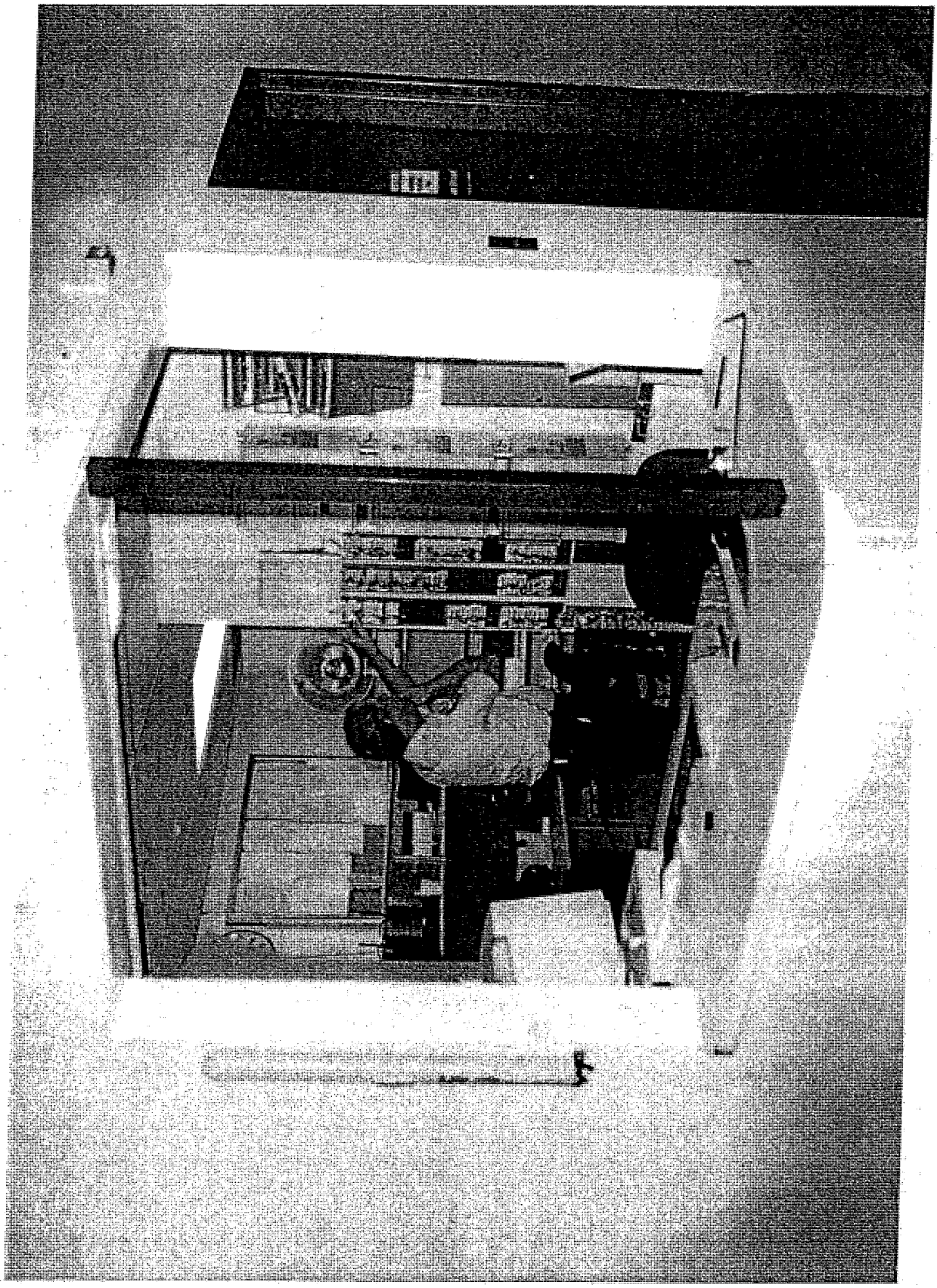
Security-Intrusion

- Relocate clinic as soon as possible
- Trim bushes & trees within 30 ft of building
- Make "guard" force a "police" force
- Upgrade security control center to PMO "standard"
  - Bullet resistant glass--pass through--hardened walls & doors
- Construct interior vestibule at back entrance to control traffic

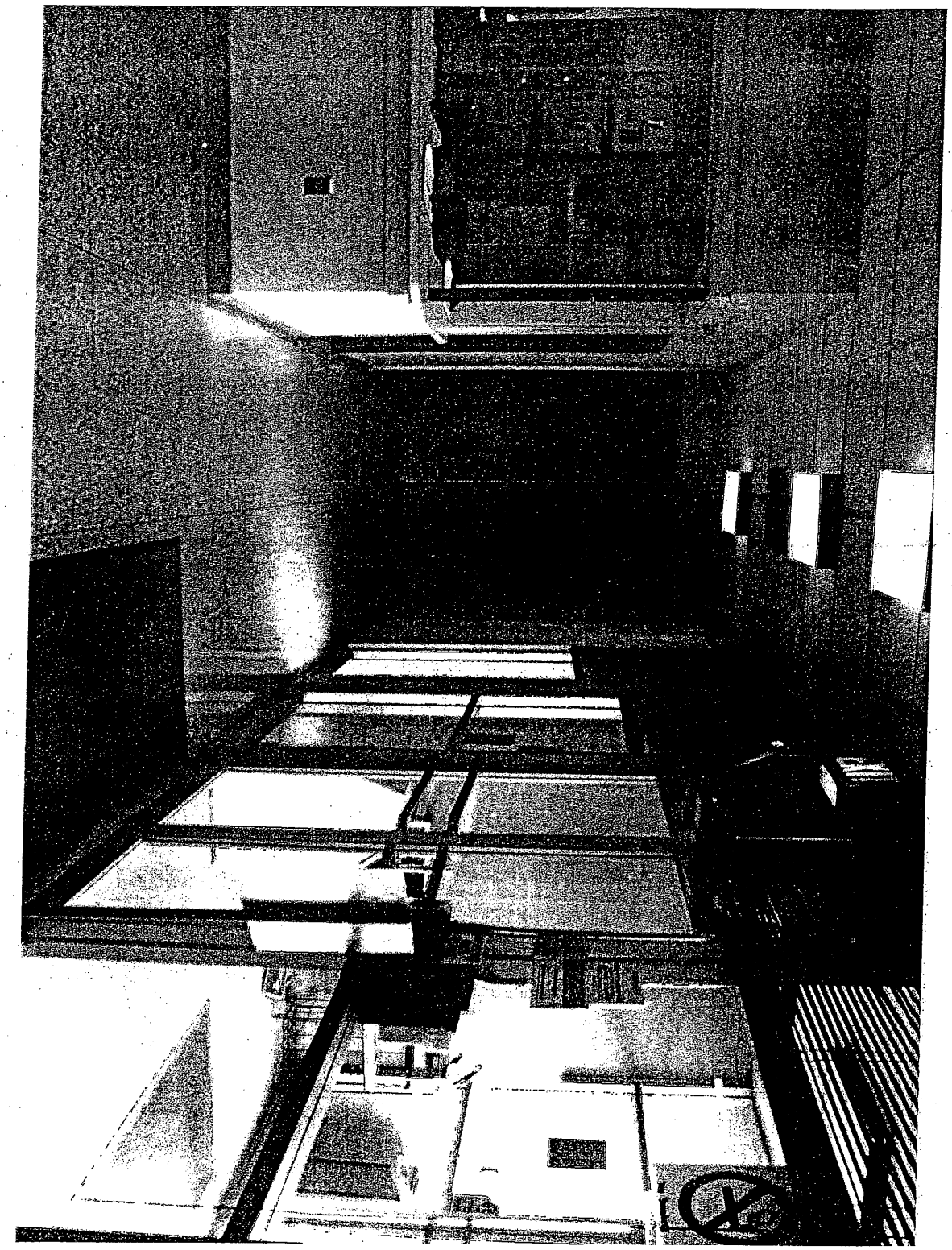
[redacted]

SMAMRIID

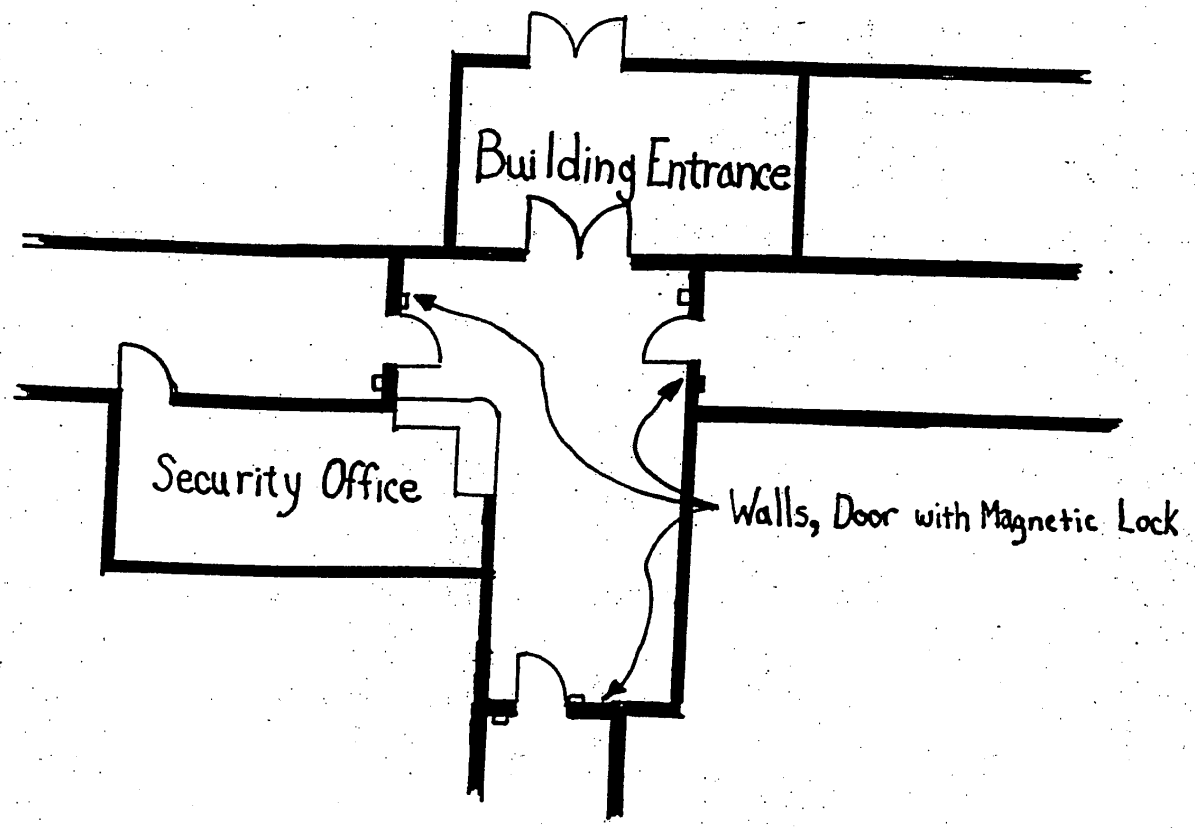
ARMY02-010574



ARMY02-010575



ARMY02-010576



Security Vestibule

ARMY02-010578

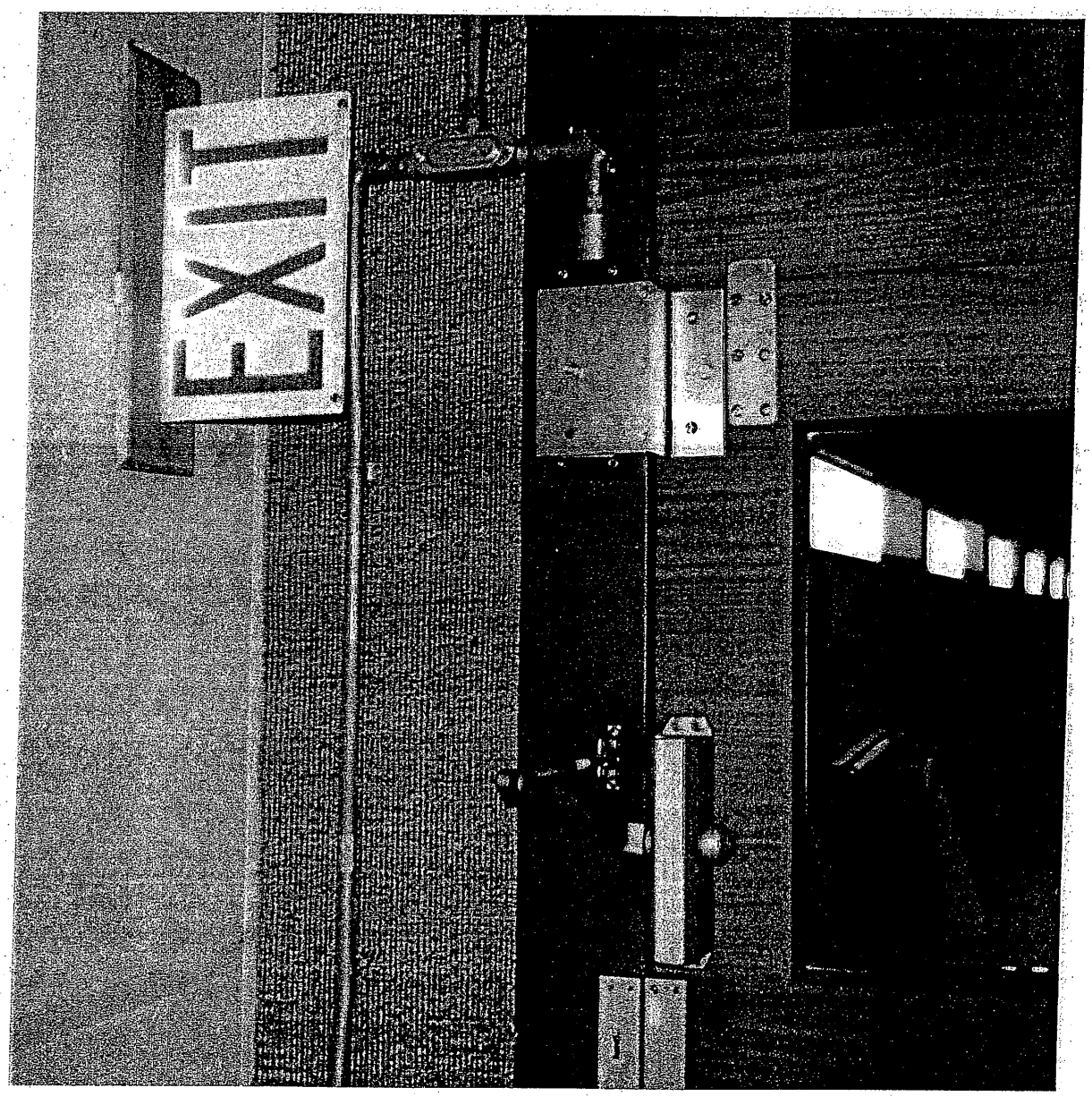
[redacted]

Security-Intrusion

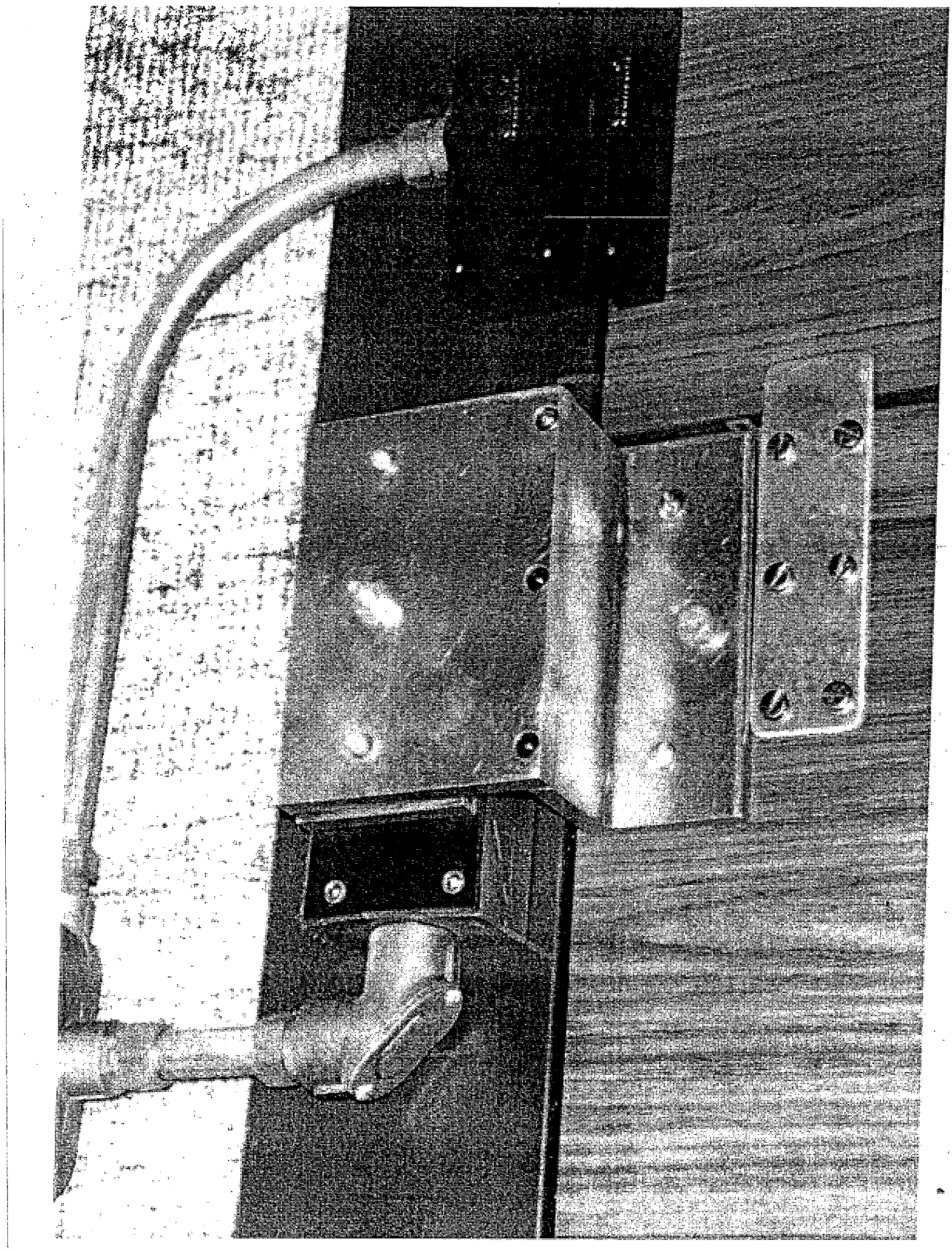
- Add additional cameras to improve surveillance capability
- Lock and alarm doors to penthouse ventilation runs
- Install "ladder locks" on roof access ladders
- Improve tamper resistant features of door magnetic devices
- Install alarms on laboratory crash doors
- Modify BSL-3 passboxes to prevent unauthorized entry/access
- Equip elevator in Bldg 1425 with a "down" key access
- Close in Bldg 1412 fire escape and alarm crash doors
- Fence in Bldgs 1412 and 1425 to restrict personnel access

[redacted] SMAMRIID [redacted]

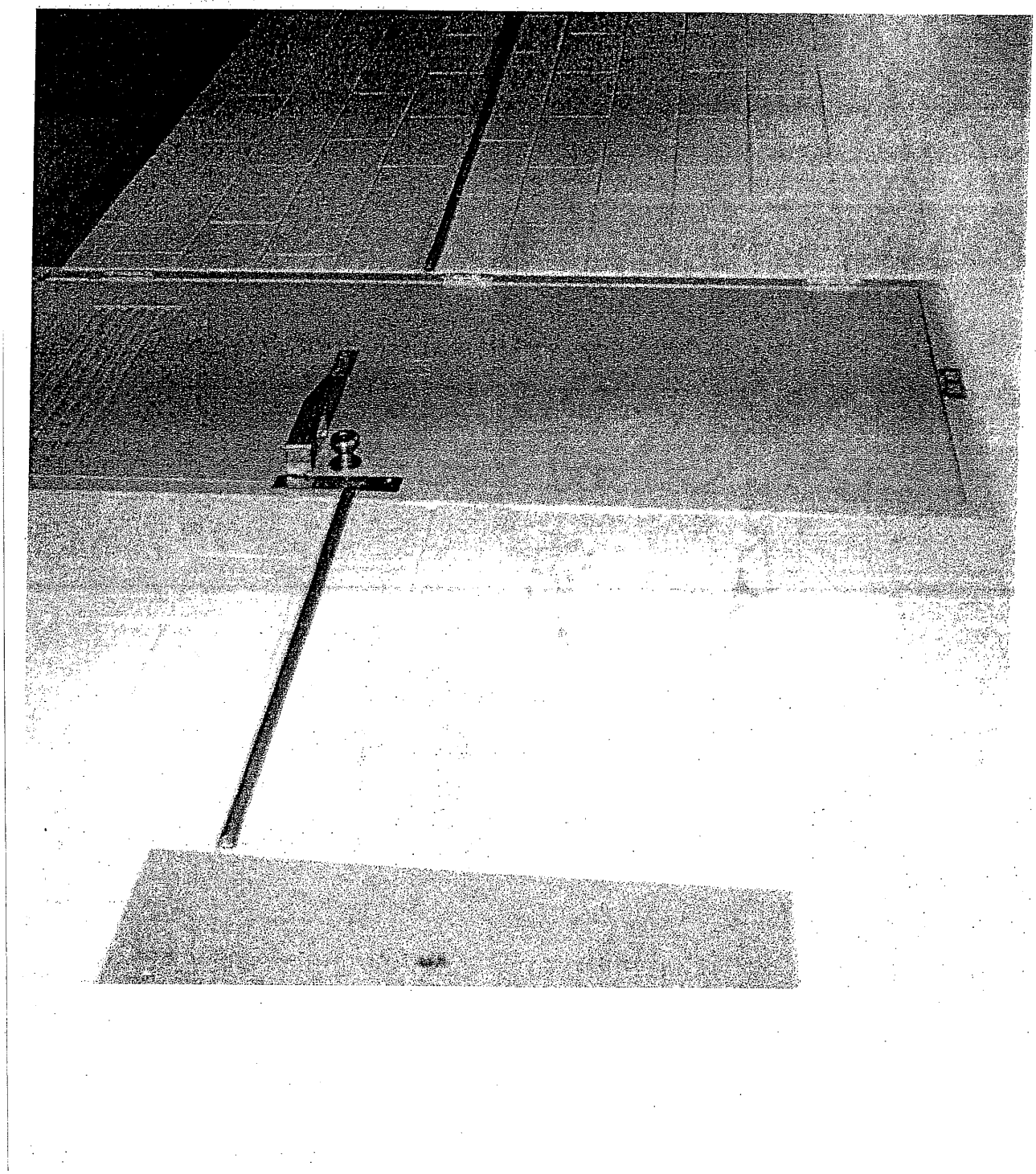
ARMY02-010579



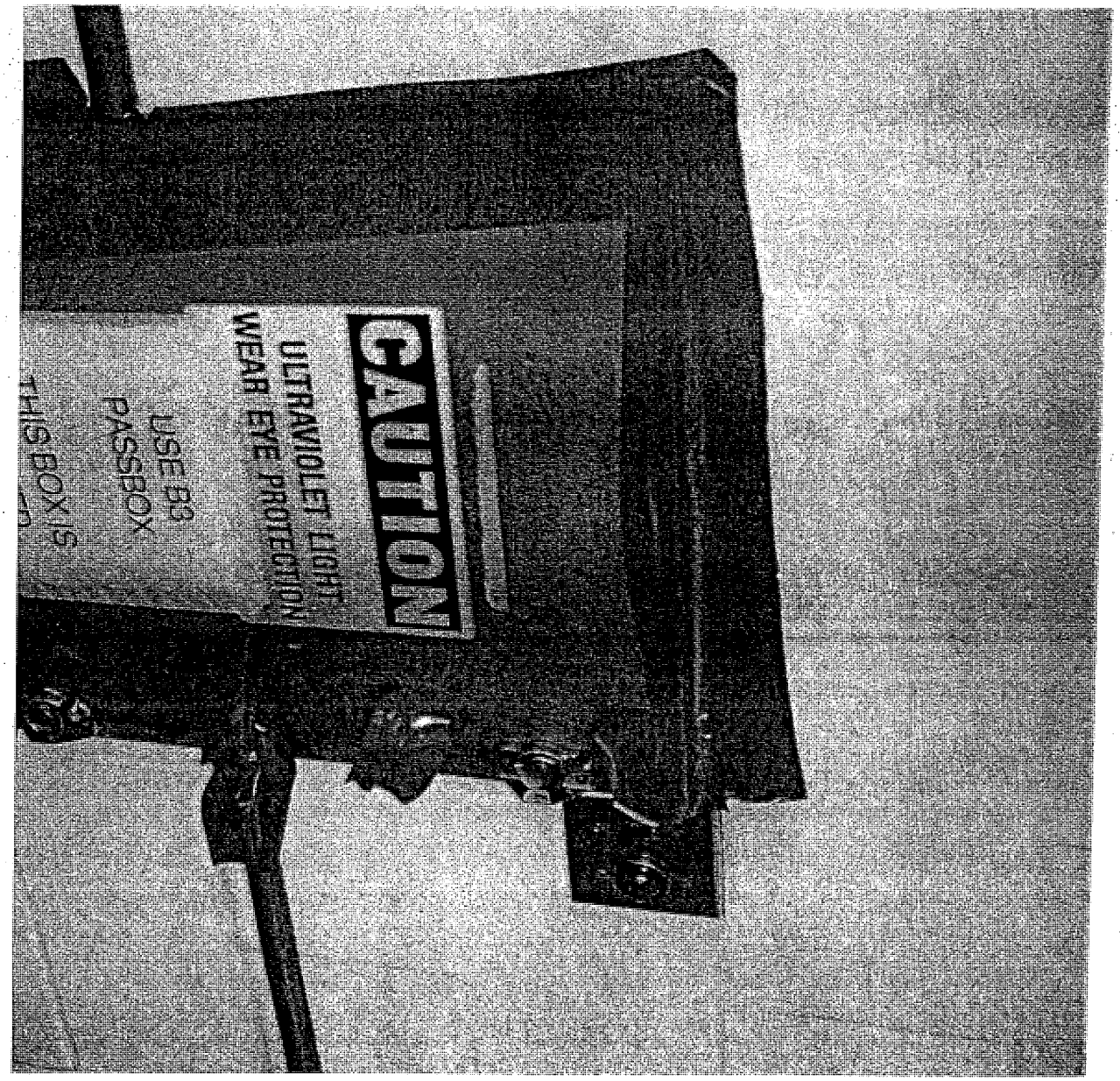
ARMY02-010580



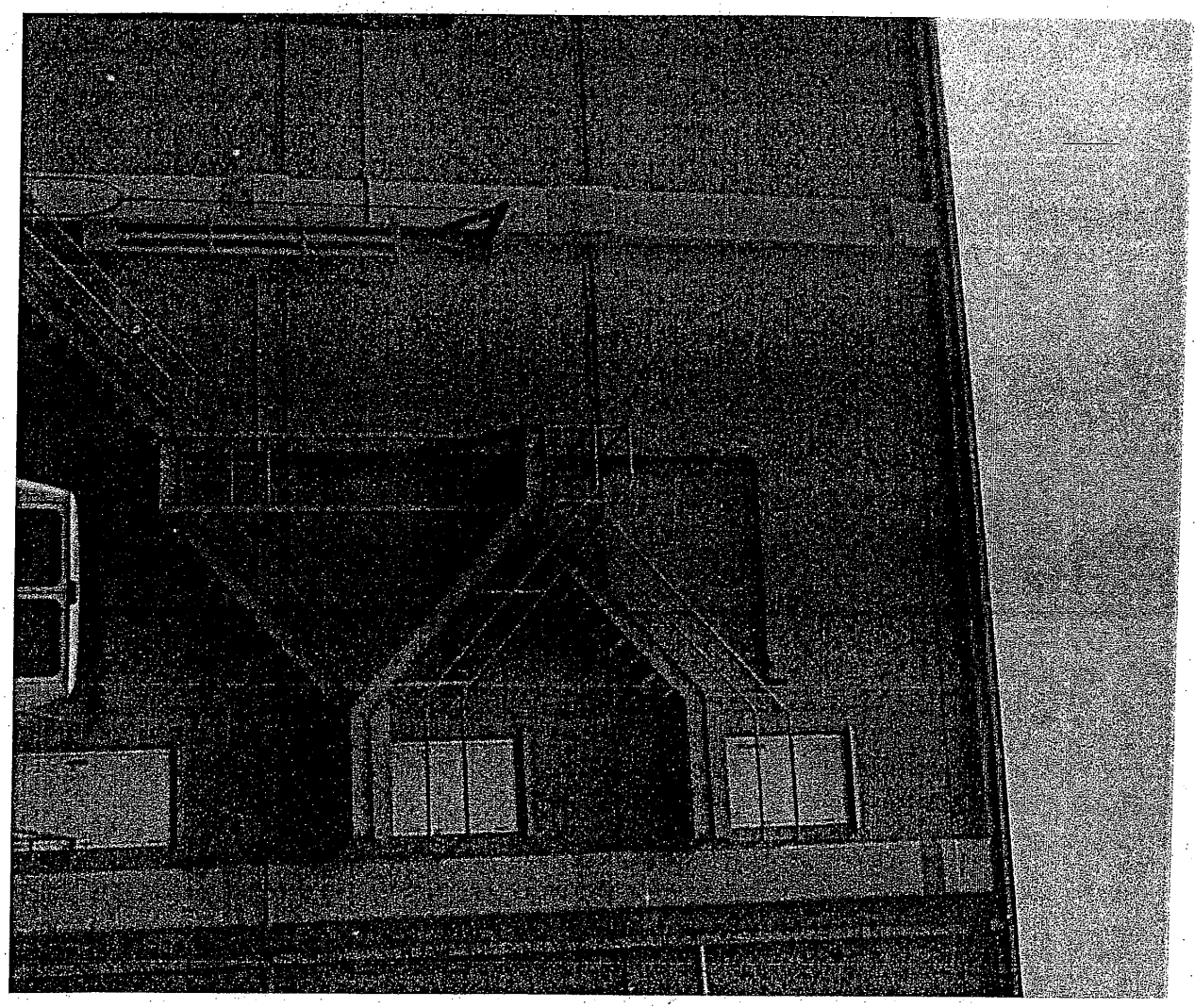
ARMY02-010581



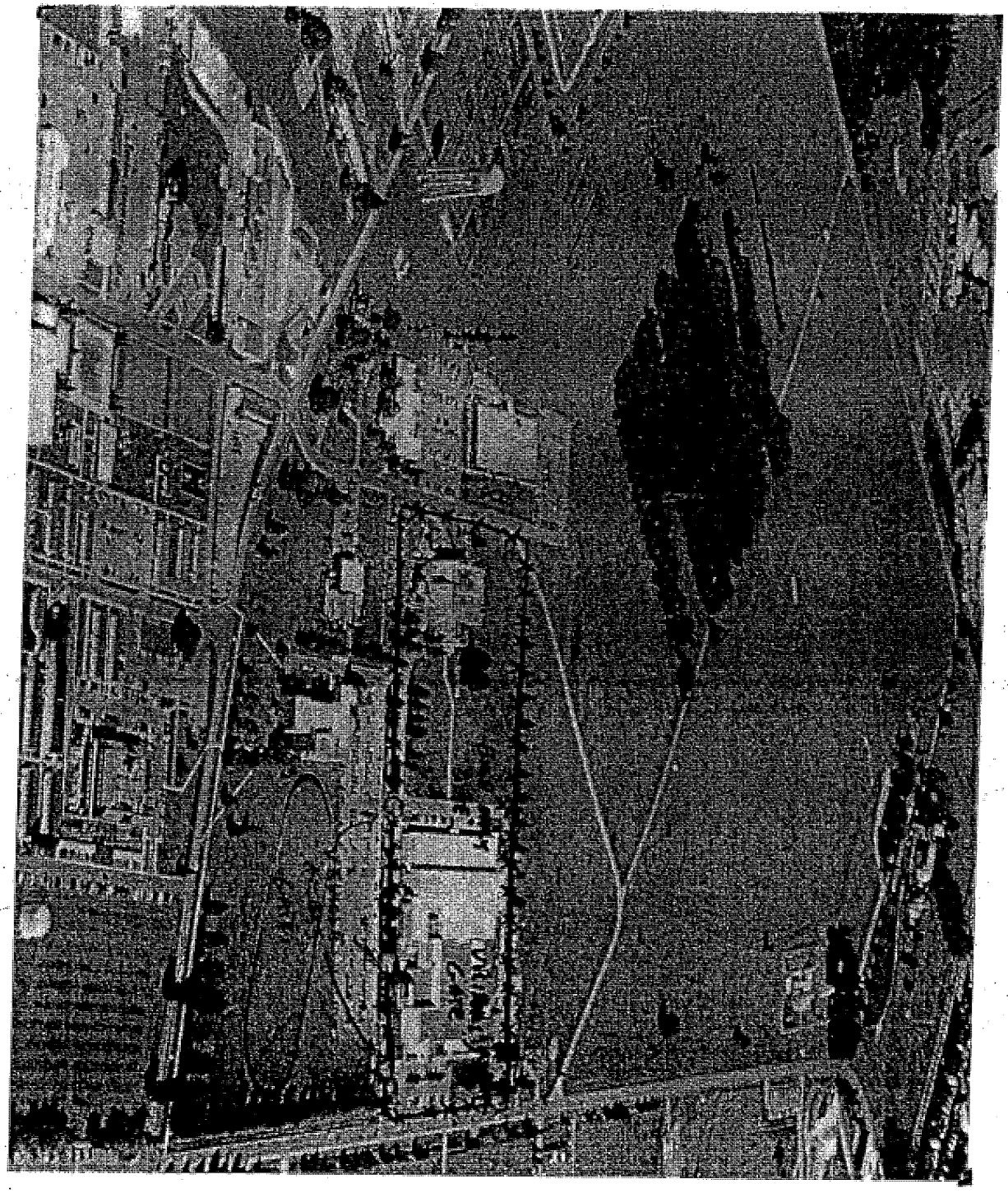
ARMY02-010582



ARMY02-010583



ARMY02-010584



ARMY02-010585

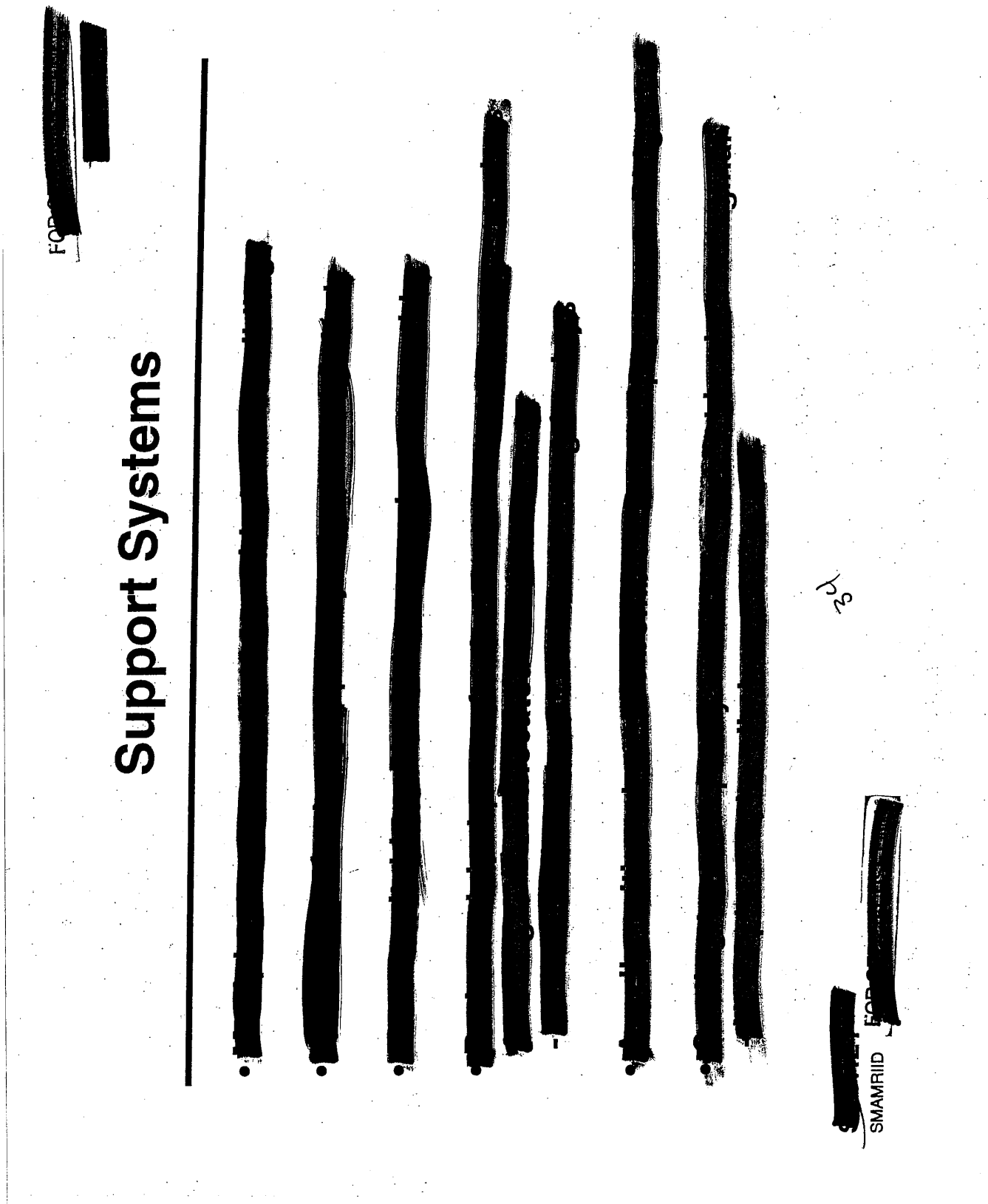
Security-People

- Challenge unbadged personnel and strangers
- Emphasize anti-piggyback policy
  - Review implementation of anti-passback system
- Implement random searches of packages & briefcases brought into buildings and all protocol volunteer luggage
- Institute duress procedure for key personnel
- Require background checks or escort all non-permanent personnel

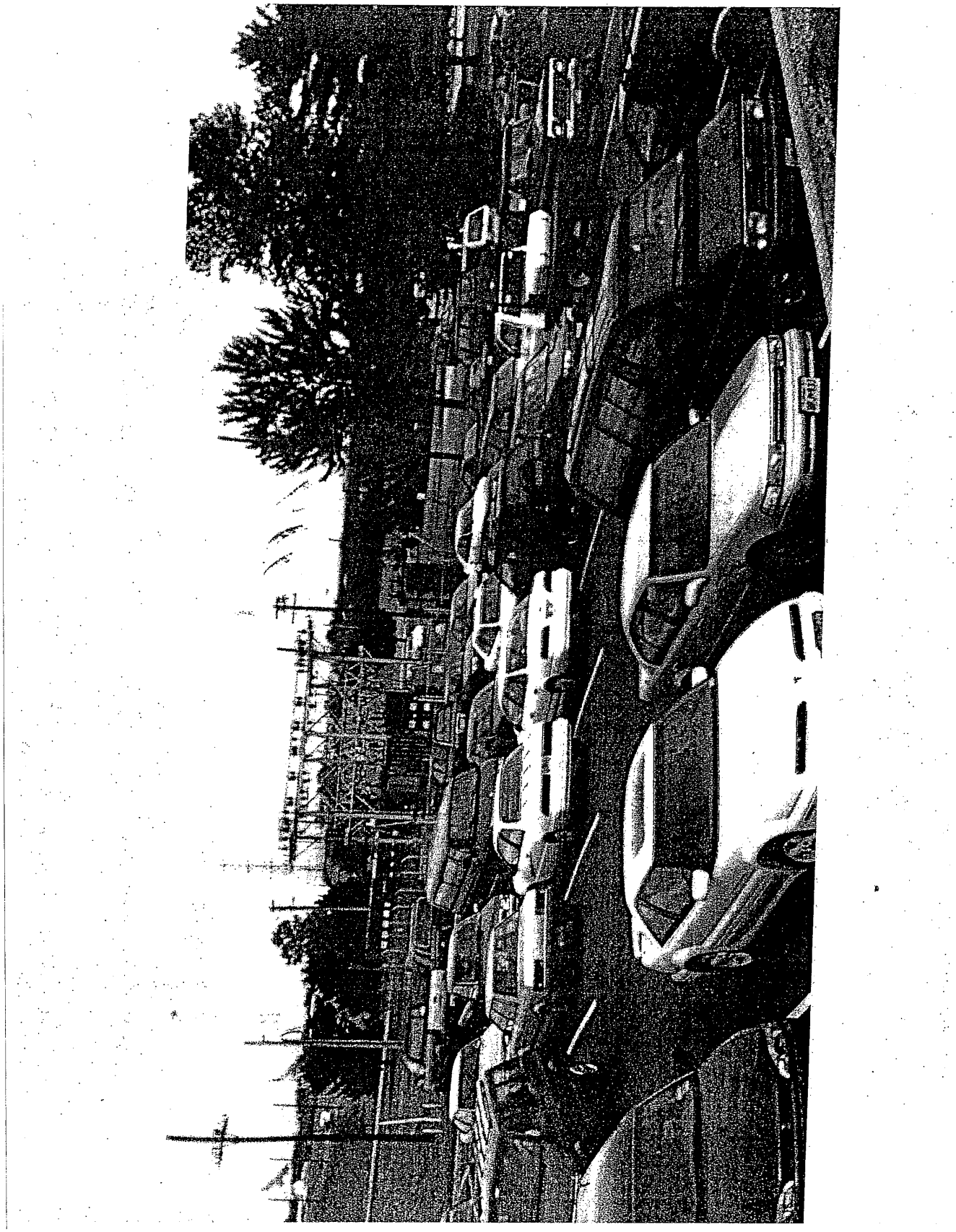
[redacted]

SMAMRIID

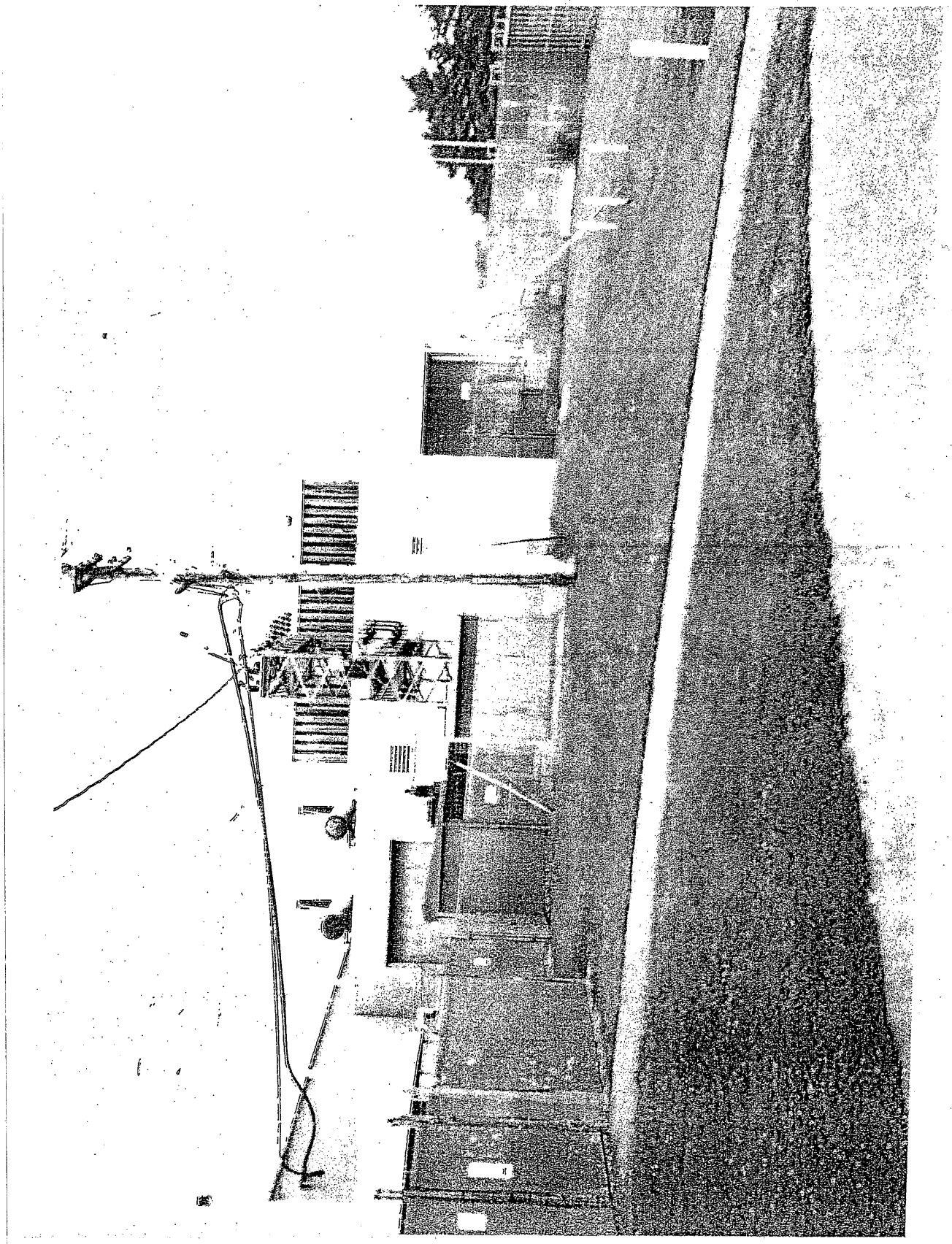
ARMY02-010586



ARMY02-010587



ARMY02-010588



ARMY02-010589

Fire Protection

- Well designed fire protection plan
  - Post fire department well trained and equipped
  - Central & remote monitoring fire alarm system
  - Integrated door control system
- Difficulties
  - No automatic fire suppression system in critical areas
  - Insufficient number of standpipe locations
  - Dumpsters located under roofs of loading docks
  - Only FDFD authorized entrance to labs in emergencies
  - Personnel not given formal emergency training
  - Fire drills not held--few escape routes marked

Lack of training detracts from an overall good system

[redacted]

SMAMRIID

ARMY02-010590

Emergency Preparedness

- Well organized and structured EP plans at both USAMRIID and the Post address most emergency situations
- Excellent support provided by Ft. Detrick
  - USAMRIID needs to carefully watch Site R planning
- Difficulties
  - Public affairs not included in plans
  - USAMRIID does not exercise emergency response plans
  - Only three channels available on Base radio net
- Helicopters overfly buildings

[redacted]

SMAMRIID

ARMY02-010591

Emergency Preparedness

Generally, emergency preparedness is not focused toward responding to a large scale or catastrophic events (i.e., destruction of Bldg. 1425 with potential agent release)

Must address full spectrum of threats

[redacted]

SMAMRIID

ARMY02-010592

Operations

- Biosafety designation of containment labs vary
  - Maintenance, safety and security have different lists
- Biosafety procedures not reviewed
- Training provided by USAMRIID to outside medical personnel is outstanding
- An inventory of agents is maintained and updated
  - Type, location and principal investigation
  - List is maintained in a single location
- Informal arrangements with CDC and chemical/biological response team should be formalized

[redacted]

SMAMRIID

ARMY02-010593

Communications (Telephones)

- Telephones connected to base network
  (Two links for 1425 - one for 1412)
  - Two STU terminals

- Disruption of communications in a crisis would be a problem

- Recommendations
  - Review of alternate communication plans (and exercises)
  - Purchases of a IMARSAT SATCOM STU III Terminal
  - Cellular phones for key staff
  - STU III terminals for key staff

Additional emphasis needed on communications

[redacted]
SMAMRIID

45

Communications (LAN)

- Standard ethernet type system (~600 nodes-10 servers)
- Not all servers supported by UPS's
- Security of the data on network is questionable
- Data back-up procedure are in place
  - Monthly backups stored on Post
  - Incremental backups stored near servers

[redacted]

SMAMRIID

ARMY02-010595

Information and Network Assurance

- USAMRIID networks are not protected from unauthorized access
- Personally owned disks easily introduced
- Files not always checked for viruses
- Virus software not current
- Hardware procurement not coordinated impacts network reliability

Information assurance needs attention

[redacted]

SMAMRIID

ARMY02-010596

Industrial Base Analysis

- Review accomplished by IASO
- Over 30 items identified as necessary to support BL4 laboratory operators
- Preliminary evaluation is that all items are off-the-shelf and commercially available
- Remaining issues are "acceptable delivery times" and long-term viability of major suppliers

[redacted]

SMAMRIID

[redacted]

Assessment of USAMRIID Perceived Risks

- Actions that jeopardize USAMRIID "open" reputation
  - Certainly a concern--issue drives security posture
- Open Post has reduced overall security
  - Yes -- however, closed post would not solve terrorist problem
- Protests or attacks by animal activists
  - Possible -- probability seems to be increasing

[redacted]

ARMY02-010598

[redacted]

Assessment of USAMRIID Perceived Risk

- **Release of infected animals**
  - **Unlikely - "Mole" or "take home a pet" a possibility**
- **Theft of agents by insiders or outsiders**
  - **Unlikely -- but possible, most likely an insider**
- **Release of agents through accidents or other causes**
  - **Possible -- increased protection from vehicle bombs required**
- **Actions by disgruntled employees**
  - **Unlikely**
- **Attacks by terrorist groups**
  - **Possible - growing presence, increased USAMRIID role**

[redacted]

SMAMRIID

45