



**DEPARTMENT OF THE NAVY**  
COMMANDER, FLEET ACTIVITIES YOKOSUKA  
PSC 473 BOX 1  
FPO AP 96349

CFAYINST 5530.9 CH-1  
N34  
5 Oct 2021

COMFLEACT YOKOSUKA INSTRUCTION 5530.9 CHANGE TRANSMITTAL 1

From: Commander, Fleet Activities Yokosuka

Subj: FLEET ACTIVITIES YOKOSUKA PHYSICAL SECURITY PLAN

Encl: (1) Revised pages 11-6, 11-8, and 11-23

1. Purpose. To publish change 1 to the basic instruction.
2. Action. Remove pages 11-6, 11-8, and 11-23 of the basic instruction and insert enclosure (1).
3. Records Management. Records created as a result of this instruction, regardless of media or format, must be managed per Secretary of the Navy Manual 5210.1 of September 2019.



M. R. JARRETT, JR

Releasability and distribution:

This change transmittal is cleared for public release and is available electronically only via CNIC Gateway CFAY website <https://g2.cnic.navy.mil/CNRJ/SitePages/CFAY.aspx>



DEPARTMENT OF THE NAVY  
COMMANDER, FLEET ACTIVITIES YOKOSUKA  
PSC 473 BOX 1  
FPO AP 96349

CFAYINST 5530.9  
N34  
12 Jan 2021

Commander, Fleet Activities Yokosuka Instruction 5530.9

From: Commander, Fleet Activities Yokosuka

Subj: FLEET ACTIVITIES YOKOSUKA PHYSICAL SECURITY PLAN

Ref: (a) DoD Instruction 2000.16, Vol. I Change 2 of 20 November 2019  
(b) DoD Manual 5200.08R Volume 3 CH-1 of 18 September 2020  
(c) DoD Manual 5200.01 Volume 2 Change 2 of 19 March 2013  
(d) UFC 4-010-01  
(e) UFC 4-020-01  
(f) UFC 4-021-02  
(g) UFC 4-022-03  
(h) UFC 4-025-01  
(i) UFC 4-215-01  
(j) OPNAVINST 5530.13C  
(k) OPNAVINST 5530.14E CH-3  
(l) NTTP 3-07.2.3  
(m) CNIC M-5530.1  
(n) CNIC M-5530.2  
(o) UG-2040-SHR  
(p) USFJINST 31-204  
(q) USFJINST 64-100  
(r) COMNAVFORJAPANINST 5500.7K  
(s) COMFLEACTINST 5700.1R  
(t) COMFLEACTINST 5800.2G  
(u) COMFLEACTINST 5530.3E  
(v) COMFLEACTINST 11101.29C  
(w) Directive-Type Memorandum 09-012

Encl: (1) Consolidated Restricted Area List

1. Purpose. To establish policies, procedures, and responsibilities for the Commander, Fleet Activities (FLEACT) Yokosuka Physical Security Plan per references (a) through (w). The concept is to implement policies and minimum standards for the physical protection of FLEACT Yokosuka personnel, operations and installation assets.

2. Cancellation. COMFLEACTINST 5530.6C, COMFLEACTINST 5530.7 and COMFLEACTINST 5532.1D. This instruction is a complete revision and should be reviewed in its entirety.

3. Scope. This instruction applies to all ashore, afloat, tenant, visiting units and personnel onboard FLEACT Yokosuka.

4. Responsibilities. While Physical Security measures remain the responsibility of each tenant activity, the Installation Commander will exercise the authority to integrate and coordinate the Physical Security measures of all commands onboard the installation. Specific responsibilities are:

a. Installation Commander. Responsible for the implementation of this instruction for Main Base, Ikego Housing Facility, Urago, Hakozaki/Azuma Island, Tsurumi OU-1 and OU-2, Nagai, and Negishi. Other Areas of responsibility are covered in individual inter or intra service support agreements.

b. Security Officer (SO). The SO reports to the Installation Commander via the Chief Staff Officer (CSO) on all matters contained within this instruction. The SO is responsible for Main Base, Ikego Housing Facility, Urago, Hakozaki/Azuma Island, Tsurumi OU-1 and OU-2, Nagai, and Negishi.

c. Assistant Security Officer (ASO). The ASO reports to and assists the SO on all matters contained within this instruction. ASO normally is assigned the duties as the Arms, Ammunition and Explosives (AA&E) Accountability Officer.

d. AA&E Accountability Officer. Installation Commander will designate in writing an individual in this position. The AA&E Accountability Officer is responsible for all AA&E accountability matters and ensuring command-wide compliance with reference (j).

e. Physical Security Officer (PSO). The FLEACT Yokosuka PSO responsibilities include but are not limited to:

(1) Manages all aspects of the command physical security program and coordinates all physical security, access control, and administrative requirements in support of the restricted areas onboard Main Base, Ikego Housing Facility, Urago, Hakozaki/Azuma Island, Tsurumi OU-1 and OU-2, Nagai, and Negishi.

(2) Coordinates Physical Security Inspections, Surveys, and site visits for FLEACT Yokosuka and other commands per requirements outlined in references (k) and (m), and upon request.

(3) Monitoring Physical Security Survey and Inspection discrepancies to ensure letters of replies and corrective action by FLEACT Yokosuka department heads or tenant CO/OICs are accomplished in a timely manner.

(4) Coordinate with the Antiterrorism Officer (ATO), Emergency Management Officer (EMO), Explosives Safety Officer (ESO), and tenant activities, all aspects requiring coordinated efforts for physical security, antiterrorism, emergency management, and AA&E.

(5) Provide logistical support for special events.

(6) Keeps the FLEACT Yokosuka SO informed of deficiencies and areas of non-compliance in the physical security program.

(7) Actively participates in the Antiterrorism Working Group (ATWG), Threat Working Group (TWG) and Antiterrorism Executive Committee (ATEC). For further guidance on ATWG, TWG and ATEC responsibilities see reference (u).

(8) Serves as the representative to the Installation Commander for all physical security matters.

f. Tenant Activity CO/OIC. All tenant activity CO/OICs will abide by the requirements outlined in this instruction. They are responsible for notifying the Installation Commander via the PSO and SO of any physical security discrepancies.

g. FLEACT Yokosuka Department heads, while under the direct supervision of the Installation Commander, are expected to comply with the requirements outlined in this instruction where applicable.

5. Contingency Plans. Refer to reference (u) and CFAYINST 3440.17B, Emergency Management Plan for all contingency plans.

6. Standard Operating Procedures and Post Orders. Refer to the Standard Operating Procedures and Post Orders for FLEACT Yokosuka Security Department.

7. Preplanned Responses. Refer to the Preplanned Responses for FLEACT Yokosuka Security Department located in reference (u) Annex C Appendix 8.

8. Coordinating Requirements. Due to the complex operating environment within the country of Japan coordinating requirements are already established in support of multiagency responses. This is not an all-inclusive list of support or coordinating requirements but is used to provide the general framework.

a. All Department of Defense (DoD) Installations and Units will follow the United States Forces Japan Instruction (USFJI) 31-203 Law Enforcement Procedures in Japan.

(1) Areas of responsibility are established to facilitate U.S. forces rapid response to incidents involving U.S. forces personnel.

(2) For areas or installations under U.S. control, the parent command or site commander has primary responsibility for law enforcement matters within the area under their control, but may enter into support agreements with other commands as needed to provide adequate response and protection. FLEACT Yokosuka has a written agreement in place for law enforcement at Yokohama North Dock (Fleet Mail Center) to be covered by U.S. Army Garrison Japan.

b. The Agreement Under Article VI of the Treaty of Mutual Cooperation and Security Between Japan and the United States of America, Regarding Facilities and Areas and the Status of United States Armed Forces in Japan is the governing instruction for coordinating requirements between the Government of Japan and the United States Government and all military branches in Japan.

c. Naval Criminal Investigative Services, Far East Field Office (NCIS FEFO) is the federal agency responsible for investigating major crimes onboard FLEACT Yokosuka. SECNAVINST 3300.2C provides guidance on the authority and responsibilities of NCIS FEFO.

9. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy Manual 5210.1 of September 2019.

10. Review and Effective Date. Per OPNAVINST 5215.17A, the FLEACT Yokosuka N34 will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and Navy policy and statutory authority using OPNAV 5215/40. The instruction will automatically expire ten years after effective date unless reissued or cancelled prior to the 10-year anniversary date, or an extension has been granted.

11. Forms. Forms are available for download from [https://navalforms.documentservices.dla.mil/formsDir/\\_SECNAV\\_5512\\_1\\_11787.pdf](https://navalforms.documentservices.dla.mil/formsDir/_SECNAV_5512_1_11787.pdf) and from CFAY VCC Homepage. [https://www.cnic.navy.mil/regions/cnrj/installations/cfa\\_yokosuka/om/security/industrial\\_security.html](https://www.cnic.navy.mil/regions/cnrj/installations/cfa_yokosuka/om/security/industrial_security.html). The complete list of required forms and their availability is contained in chapter 12 of this instruction.



M. R. JARRETT, JR

Releasability and distribution:

This instruction is cleared for public release and is available electronically only via CNIC Gateway CFAY website <https://g2.cnic.navy.mil/CNRJ/SitePages/CFAY>

**Table of Contents**

**CHAPTER 1 AREA SECURITY** ..... 1-1

    1 General ..... 1-1

    2 Critical Infrastructure ..... 1-1

    3 Priority of Response ..... 1-1

    4 Waterfront Security ..... 1-1

    5 Electronic Harbor Security Systems (EHSS) ..... 1-1

**CHAPTER 2 PHYSICAL SECURITY INSPECTIONS AND SURVEYS** ..... 2-1

    1 General ..... 2-1

    2 Information Requirements ..... 2-1

    3 Physical Security Inspections (PSI) ..... 2-2

    4 Physical Security Surveys (PSS) ..... 2-2

    5 PSI/PSS Tracking System ..... 2-3

    6 PSI Requests ..... 2-3

    7 Physical Security Inspector Requirements ..... 2-3

    8 Reviewing Requirements ..... 2-4

    9 Corrective Action Plan (CAP) and Plan of Action and Milestone (POA&M) ..... 2-4

    10 Waivers and Exemptions ..... 2-5

**CHAPTER 3 RESTRICTED AREA CONTROL MEASURES** ..... 3-1

    1 Purpose ..... 3-1

    2 Restricted Area Identification ..... 3-1

    3 Access Control for Restricted Areas ..... 3-1

    4 Minimum Security Requirements for Classified Material ..... 3-3

**CHAPTER 4 MATERIAL CONTROL MEASURES** ..... 4-1

    1 General ..... 4-1

    2 Definitions ..... 4-1

    3 Policy ..... 4-1

    4 Responsibilities ..... 4-1

    5 Controlled Substances Inventory ..... 4-2

    6 Security Requirements for “R”-Coded Items at Base/Installation Supply Level or Higher ..... 4-2

    7 Security Requirements for “Q”-Coded Items at Base/Installation Supply Level or Higher ..... 4-2

    8 Security Requirements for “R” and “Q”-Coded Items Below Base and Installation Level ..... 4-2

    9 Outgoing Materials and Supplies ..... 4-2

|   |            |
|---|------------|
| <b>CHAPTER 5 PROTECTIVE BARRIERS, FENCES AND SIGNS .....</b>                | <b>5-1</b> |
| 1 Protective Barriers.....  | 5-1        |
| 2 Port Security Barrier (PSB).....  | 5-2        |
| 3 Fences .....  | 5-2        |
| 4 Walls .....   | 5-2        |
| 5 Security Lattice .....  | 5-2        |
| 6 True Wall Requirements .....  | 5-3        |
| 7 Identification .....  | 5-3        |
| 8 Signs and Posting of Boundaries .....                                     | 5-4        |
| 9 Clear Zones .....   | 5-5        |
| <b>CHAPTER 6 INSTALLATION ENTRY CONTROL POINTS .....</b>                    | <b>6-1</b> |
| 1 General.....  | 6-1        |
| 2 Entry Control Points onboard Main Base .....                              | 6-1        |
| 3 Entry Control Points onboard Ikego Housing Facility.....                  | 6-2        |
| 4 Entry Control Points onboard Hakozaki and Azuma Island .....              | 6-2        |
| 5 Entry Control Points onboard Tsurumi OU-1 and OU-2.....                   | 6-2        |
| 6 Entry Control Points onboard Urago.....                                   | 6-2        |
| 7 Policy on Searching Military and Privately Owned Vehicles at the ECP..... | 6-3        |
| 8 Actual or Attempted Unauthorized Access.....                              | 6-3        |
| <b>CHAPTER 7 PROTECTIVE LIGHTING SYSTEMS .....</b>                          | <b>7-1</b> |
| 1 Protective Lighting Systems .....   | 7-1        |
| 2 Technical Aspects .....   | 7-2        |
| 3 Protection of Controls and Switches .....                                 | 7-2        |
| 4 Other Lighting Systems in Use .....                                       | 7-2        |
| 5 Inspection and Maintenance Responsibilities .....                         | 7-3        |
| 6 Commercial and/or Alternate (Emergency) Power Failure.....                | 7-3        |
| 7 Emergency Lighting System.....  | 7-4        |
| <b>CHAPTER 8 ELECTRONIC SECURITY SYSTEMS (ESS) .....</b>                    | <b>8-1</b> |
| 1 General.....  | 8-1        |
| 2 Intrusion Detection Systems (IDS) .....                                   | 8-1        |
| 3 Responsibilities for IDS .....  | 8-1        |
| 4 Prior Installed Equipment .....   | 8-2        |
| 5 IDS Waivers/Exceptions .....  | 8-2        |

|  |             |
|--|-------------|
| 6 Types of Alarm Activations .....   | 8-2         |
| 7 Alarmed Facilities .....   | 8-3         |
| 8 IDS Failures and Mandatory Minimum Mitigation Measures .....                                 | 8-4         |
| 9 Installation, Monitoring and Maintenance .....   | 8-5         |
| 10 IDS Access List Procedures .....  | 8-5         |
| 11 IDS Testing Requirements .....  | 8-5         |
| 12 Navy Security Force (NSF) Response to IDS .....   | 8-6         |
| 13 Facility Custodians Response to IDS Alarm Activations .....                                 | 8-6         |
| 14 IDS Standardization .....   | 8-7         |
| 15 IDS Support .....   | 8-7         |
| 16 Closed Circuit Television (CCTV) .....  | 8-7         |
| <b>CHAPTER 9 PROTECTION OF ARMS, AMMUNITION AND EXPLOSIVES (AA&amp;E)</b> .....                | <b>9-1</b>  |
| 1 General .....  | 9-1         |
| 2 Responsibilities .....   | 9-1         |
| 3 Designation of a Firearms storage Facility .....   | 9-1         |
| 4 AA&E Storage Facility Construction .....   | 9-2         |
| 5 Ordnance Magazines Entry/Exit .....  | 9-2         |
| 6 Padlocks and Combinations Locks for AA&E Vault Doors and Containers .....                    | 9-3         |
| 7 Security Checks .....  | 9-3         |
| 8 Unattended AA&E .....  | 9-4         |
| 9 Lost, Stolen, Unaccounted for, or Recovered AA&E .....                                       | 9-4         |
| 10 Annual AA&E Screening .....   | 9-4         |
| 11 AA&E Inventories .....  | 9-5         |
| 12 Anti-pilferage Seals Program .....  | 9-6         |
| 13 AA&E Key and Lock Control .....   | 9-6         |
| 14 Combination Changes .....   | 9-8         |
| 15 Firearms and FLEACT Yokosuka Facilities .....   | 9-8         |
| 16 Sobriety While Carrying and Handling Weapons .....  | 9-9         |
| 17 Domestic Violence .....   | 9-9         |
| 18 Incidents Causing Revocation for Carrying or Assigned as Custodian to AA&E Facilities ..... | 9-10        |
| <b>CHAPTER 10 KEY AND LOCK CONTROL PROGRAM</b> .....   | <b>10-1</b> |
| 1 Purpose .....  | 10-1        |
| 2 Discussion .....   | 10-1        |



|  |             |
|--|-------------|
| 3 Scope.....   | 10-1        |
| 4 Responsibilities.....  | 10-1        |
| 5 Procedures.....  | 10-3        |
| 6 Locks.....   | 10-6        |
| 7 Inventories.....   | 10-7        |
| 8 Action.....  | 10-8        |
| 9 Forms.....   | 10-8        |
| <b>CHAPTER 11 INSTALLATION ACCESS CONTROL POLICY.....</b>                | <b>11-1</b> |
| 1 Purpose.....   | 11-1        |
| 2 Scope.....   | 11-1        |
| 3 General.....   | 11-1        |
| 4 Forms.....   | 11-6        |
| 5 Definitions of Authorized Personnel.....                               | 11-6        |
| 6 Escort Privileges.....   | 11-10       |
| 7 Satellite Area Access.....   | 11-13       |
| 8 Unofficial Visitor Requirements.....                                   | 11-14       |
| 9 Official Visitor Requirements.....                                     | 11-16       |
| 10 Contingency Plan for Non-DBIDS Use.....                               | 11-20       |
| 11 Multi-Installation Access.....  | 11-21       |
| 12 Designated Third Country Nationals (DTCN).....                        | 11-22       |
| 13 Single Source Coordinator.....  | 11-23       |
| 14 DBIDS Categories.....   | 11-25       |
| 15 Denial of Access.....   | 11-25       |
| 16 Temporary Vehicle Access.....   | 11-27       |
| 17 Violation Policy.....   | 11-29       |
| 18 Procedures in Case of Loss of Credentials.....                        | 11-30       |
| 19 Authorized Identification For Visitors.....                           | 11-31       |
| 20 Authorized Identification Cards of Use at Visitor Control Center..... | 11-33       |
| <b>CHAPTER 12 FORM LISTING.....</b>                                      | <b>12-1</b> |

## Chapter 1

### AREA SECURITY

1. General. All property that is within the perimeter fence line or property line belonging to the U.S. Government and under the Installation Commander's control is designated as controlled areas and protected by the Naval Security Forces (NSF). Special protective measures must be taken to protect areas, buildings and other structures considered critical.
2. Critical Infrastructure. Critical Infrastructure is defined as facilities, systems and functions that are highly sophisticated and complex. They include human assets and physical and cyber systems that work together in processes that are highly interdependent. They also consist of key nodes that, in turn, are essential to the operation of the critical infrastructures in which they function. Examples include computer network systems, defense switchboard networks, potable water systems, power systems, utility services, communications systems, intelligence gathering systems and any other asset designated by the Installation Commander, in writing and on the Installation Consolidated Restricted Area List, (enclosure (1)).
3. Priority of Response. Assets that are designated as critical will be protected in a cascading manner, i.e. flowing from highest priority to lowest priority. Assets will be protected based on their importance to the defense of the United States of America first and work their way downward to the local level. Assets will be prioritized in the following order: Level 3 Restricted Areas that are Assets Vital to National Security, Critical Infrastructure, Inherently Dangerous Property, and then all other Level 3 Restricted Areas. Level 2 Restricted Areas that are Assets Vital to National Security, Critical Infrastructure, Inherently Dangerous Property, and then all other Level 2 Restricted Areas. Level 1 Restricted Areas that are Assets Vital to National Security, Critical Infrastructure, Inherently Dangerous Property, and then all other Level 1 Restricted Areas. Refer to the Installation Consolidated Restricted Area List, (enclosure (1)), for Level 1 through 3 restricted areas.
4. Waterfront Security. Waterfront Security is the responsibility of FLEACT Yokosuka Security, and specifically the Harbor Patrol Unit. See reference (u) for all guidance regarding protection of assets moored or anchored at FLEACT Yokosuka.
5. Electronic Harbor Security Systems (EHSS). EHSS provides surveillance capability to FLEACT Yokosuka. EHSS provides both Radio Detection and Ranging, thermal and visual imaging capability as well a tracking, identifying and observing contacts of interest. EHSS will also be used to provide surveillance of waterways adjacent to afloat assets at FLEACT Yokosuka when possible. See reference (u) for detailed guidance on the operation of EHSS.

## Chapter 2

### PHYSICAL SECURITY INSPECTIONS AND SURVEYS

1. General. Physical Security Surveys (PSS) and Physical Security Inspections (PSI) must be conducted on all normally inhabited facilities as well as the following:
  - a. Arms, Ammunition, and Explosives (AA&E) storage facilities per reference (b).
  - b. Exchange and commissary facilities.
  - c. Storage facilities containing sensitive and/or high value materials.
  - d. Activities possessing restricted areas and facilities and mission-critical areas, contained in enclosure (1).
  - e. The office, headquarters, or residence (if applicable) of the installation command staff and any local or regional senior leadership that regularly works or resides on the installation. At a minimum FLEACT Yokosuka will conduct PSSs and PSIs on all admiral's residences.
2. Information Requirements. The PSI and PSS will evaluate the following:
  - a. Threat assessment procedures.
  - b. Security forces, including types, availability, training, equipment and guard orders.
  - c. Compliance with access control procedures.
  - d. Control of visitors and hand-carried items.
  - e. Use of Physical Security equipment.
  - f. Security lighting.
  - g. Control, issuance and accountability of keys and locks.
  - h. Identification of critical areas and facilities.
  - i. Processes used to track Physical Security work orders and vulnerability mitigation efforts.
  - j. Deviations (waivers and exceptions) to policy.
  - k. Physical Security surveys will include:

- (1) Executive summary.
- (2) Detailed assessment of the installation's security posture.
- (3) Recommended application of resources in a prioritized manner for the reduction of vulnerabilities.
- (4) Use of exhibits to include; photographs of the asset and any identified discrepancies, and any other amplifying documentation deemed necessary.
- (5) Mission of the responsible unit.
- (6) Potential threat(s) to the asset.
- (7) Comparison of findings from previous surveys and inspections.

3. Physical Security Inspections (PSI). PSI are an in depth formal assessment of an activity's physical security program that includes antiterrorism and force protection. The intent of these inspections are to inform the Installation Commander and tenant activities on what needs protecting, what security measures are in effect and what areas require improvement.

- a. PSI provide the Installation Commander with a basis for determining security priorities.
- b. PSI will be conducted every two years. FLEACT Yokosuka conducts PSI every even numbered fiscal year.
- c. FLEACT Yokosuka also provides a Design Criteria Workbook from reference (e) during the PSI. This workbook contains the Asset Value, Threat Likelihood and Level of Protection for the inspected asset.

(1) Any asset that has a Threat Likelihood of .51 or greater is deemed inadequately protected.

(2) Assets deemed inadequately protected will be re-inspected every six months until the asset is brought within acceptable standards of .50 or less.

d. Physical Security Inspectors will be granted access to Navy units, activities, records, and information on a "need-to-know" basis, consistent with the inspector's clearance for access to classified defense information and provisions of applicable DoD and Navy policy.

4. Physical Security Surveys (PSS). PSS are a formal assessment of an activity's physical security program however, it is less in depth than the PSI and is focused on progression from the prior PSI.

a. PSS will be conducted every two years. FLEACT Yokosuka conducts PSS every odd numbered fiscal year.

b. During the PSS the Design Criteria Workbook from the prior PSI will be reevaluated.

(1) If no changes are identified with the tenant activities physical security program, then the Design Criteria Workbook from the PSI is not required to be updated.

(2) If there are changes identified with the tenant activities physical security program, the Design Criteria Workbook from the PSI will be updated.

5. PSI/PSS Tracking System. All required and requested PSI/PSS will be tracked in a locally generated Excel database. The PSO is responsible for ensuring all PSI/PSS tracking requirements are met and updated in the excel database as appropriate.

6. PSI Requests. FLEACT Yokosuka Physical Security, upon request from a tenant activity, will conduct a PSI of stand-alone facilities and special areas aligned to a CNIC installation.

a. Commands can request these inspections by emailing the Physical Security Distro List at [M-YO-CFAYPHYSEC@OCONUS.NAVY.MIL](mailto:M-YO-CFAYPHYSEC@OCONUS.NAVY.MIL) with the following information:

(1) Asset name and location.

(2) Activity name or responsible activity.

(3) Point of contact information.

(4) Reason for request.

#### 7. Physical Security Inspector Requirements

a. Inspectors conducting PSI or PSS must meet the following criteria:

(1) Be qualified as a Master-at-Arms or GS-0080.

(2) Be an E-6 and senior or be a civilian employee who meets the current General Schedule-0080 Physical Security qualification standard for the grade assigned to the position. Requirement can be waived to E-5 by Region Security Officer.

(3) Complete the Conventional Physical Security Course conducted by United States Army Military Police School, Federal Law Enforcement Training Center, Physical Security Course or other CNIC N34 approved courses that trains the individual to be a Physical Security inspector. This may be waived by the Region Security Officer based on individual's current training. Blanket waivers based on experience or rank will not be granted.

(4) Be cleared for access to SECRET national defense information.

(5) Physical Security inspectors will not engage in illegal or dangerous conduct that demonstrates security weaknesses. Inspections may be unannounced but will not unnecessarily interfere or disrupt unit mission execution.

b. Tenant activities using their own personnel to conduct PSI or PSS must submit documentation of all above requirements when submitting their PSI or PSS to the FLEACT Yokosuka Physical Security.

(1) If a tenant activity has their own qualified personnel conducting the PSI or PSS, they must be completed and submitted to FLEACT Yokosuka Physical Security no later than the first of September of every fiscal year.

(2) If the tenant activity does not submit the appropriate documentation of above requirements, the PSI or PSS will be rejected and FLEACT Yokosuka Physical Security will conduct a PSI or PSS prior to the end of the fiscal year.

8. Reviewing Requirements. All PSI and PSS must be reviewed and signed by the Installation Commander.

a. All PSI and PSS are routed through the PSO to the SO for review and signature.

(1) Upon review SO will sign the PSI or PSS, and route to the Installation Commander for final review and approval.

(2) Upon final approval from the Installation Commander, the PSI or PSS will be returned to the PSO.

(3) PSO will return the approved PSI or PSS to the owning activity along with a Corrective Action Plan (CAP) template.

b. The approved and signed PSI or PSS will be maintained on file for a minimum of three years.

9. Corrective Action Plan (CAP) and Plan of Action and Milestone (POA&M). Upon receipt of approved PSI or PSS, tenant activities or FLEACT Department Heads will provide a report of corrective actions taken to their appropriate chain of command and to the PSO.

a. CAPs are required to be returned to the PSO with a POA&M generated by the inspected activity.

b. Any deficiency that is identified as a vulnerability or could result in a loss of life requires immediate compensatory measures to be put in place by the inspected activity.

(1) The inspected activity is required to provide written documentation to the PSO within five working days on the compensatory measures that will be taken until the repairs or work can be completed.

(2) Deficiencies requiring correction beyond the inspected unit's capabilities must be immediately reported up the Chain of Command via the PSO. Compensatory measures must be deployed until the work order can be completed. Compensatory measures will be documented in the pertinent PSI/PSS and reported up the Chain of Command via the PSO.

c. All PSI/PSS, CAP, and POA&M will be reviewed during Criticality Assessments, Vulnerability Assessments, and Threat Assessments, the results of which will be used in the Risk Analysis/ Management Process through installation working groups (ATWG, TWG, ATEC)

#### 10. Waivers and Exemptions

a. The SO will act as FLEACT Yokosuka's point of contact for submission of all waivers and exceptions related to physical security.

b. All commands within FLEACT Yokosuka will submit all waivers and exemptions to the Installation Commander via the SO.

c. FLEACT Yokosuka Physical Security and the tenant activity needing the waiver or exemption will identify necessary additional physical security measures and codify the requirement in a memorandum of agreement until the vulnerabilities are corrected and identify a timeline for repair or correction.

d. All waivers and exemptions will be documented in Enterprise Protection Risk Management (EPRM). Any activity requesting or directed to submit waivers will be part of the effort and assist in data collection and mitigation efforts.

### Chapter 3

#### RESTRICTED AREA CONTROL MEASURES

1. Purpose. Outline recommendations and requirements for access control to all restricted areas onboard Main Base, Ikego Housing Facility, Urago, Hakozaki/Azuma Island, Tsurumi OU-1 and OU-2, Nagai, and Negishi in order to detect and prevent the introduction of prohibited items (firearms, explosives, drugs, etc.) and the unauthorized removal of government property or material

2. Restricted Area Identification. Restricted area definitions are outlined in depth in reference (k).

a. Tenant activities and FLEACT Yokosuka department heads are responsible for identifying all restricted areas within their purview and ensuring that those restricted areas are published in their Physical Security Plan per reference (m).

b. Tenant Activities will submit a Restricted Area Designation Letter to the Installation Commander via the PSO no later than the first of December every calendar year.

(1) FLEACT Yokosuka Physical Security will consolidate all known Restricted Areas onto the Installation Consolidated Restricted Area List and route to the Installation Commander for review and signature.

(2) The Installation Consolidated Restricted Area List will be published in reference (u) and is (enclosure (1)) of this instruction.

3. Access Control for Restricted Areas. All restricted areas must have access control measures in place per references (k) and (l).

a. At a minimum all Restricted Areas containing classified material or AA&E will utilize an Authorized Access List (AAL) signed by the appropriate authority and posted on the interior of the restricted area for entry into the restricted area. This list will be easy to find but not be visible from the exterior of the protected space. All personnel granted unescorted access to a restricted area containing classified material or AA&E will have a need for access and be screened as required by their supervisor, security managers, or appropriate authority prior to being placed on the AAL.

b. Personnel Access to restricted areas will be granted as follows:

(1) Unit Personnel on the AAL will have unescorted access. Unit Personnel not on the access list will be treated like visitors.



(2) Visitors will have a legitimate need for access and be escorted at all times.

(a) A visitor log will be used to track personnel entry and exit and must contain the date, time entered, command they are attached to, nationality, visitor name and signature, purpose of visit, escort name and signature and departure time. It is recommended that a badging system be used in conjunction with the visitor log.

(b) If the visitor does not have the appropriate security clearance and an in-brief with a need to know for classified information then the space must be sanitized prior to the visitor entering to prevent spillage.

(3) Maintenance personnel entering a Restricted Area will meet the same requirements as visitors but be granted access to the systems they are repairing only. They must have a Work Order and coordinate access to the space prior to entry.

(4) Contractor personnel can be placed on the AAL if they meet the security requirements and have a need to access the space and material. Contractors who are not granted unescorted access will meet the same requirements as a visitor.

(5) In the event of an emergency, the Restricted Area occupants will make every attempt, without endangering their life, to secure classified material and sanitize the area prior to Emergency Response Team arrival.

(a) Emergency Responders will not be hindered in their response and be given full access to the spaces necessary for preservation of life or to protect the assets, unless a written memorandum of agreement or higher headquarters guidance has been posted restricting Emergency Responses.

(b) In the event of a life-threatening emergency or in the performance of law enforcement any first responder may make forced entry into a space. Every attempt will be made, if feasible, before destructives means are taken.

(c) Coordination between the activity responsible for the space and first responders is necessary, with special consideration taken for AA&E spaces to ensure safety and prevent mishaps.

(d) If spillage occurs as a result of an Emergency Response the restricted area tenants can request the names of all personnel involved from the on scene response for documentation purposes and to complete Non-Disclosure Agreements or other incident documents needed.

c. It is the responsibility of all activities to identify and codify policies and procedures on hand carried items entering their restricted areas. The extent and requirements will be determined by appropriate governing instructions for the assets and level of classification for the space being entered. All personnel who are not on the AAL should have an inspection of their hand-carried items prior to entering and exiting any restricted area.

d. Vehicle access to restricted areas will be granted as follows:

(1) All government vehicles entering restricted areas will be occupied by authorized personnel only, all identification cards will be checked and access lists verified if accessing a secured compound or parking area.

(2) All privately owned vehicles (POVs) will only be allowed access to restricted areas if approved by the appropriate authority. All POVs entering restricted areas will be occupied by authorized personnel, all identification cards will be checked and access lists verified if accessing a secured compound or parking area.

(3) All Emergency vehicles (Security, Fire and Medical) will be granted access to restricted areas in the performance of their duties, and are exempt from all pass or badging requirements.

4. Minimum Security Requirements for Classified Material. At a minimum the following assets will be protected by higher directives:

a. Top Secret information will be stored:

(1) In a GSA-approved security container with one of the following supplementary controls:

(a) An employee cleared to at least the Secret level will inspect the security container once every 2 hours.

(b) The location that houses the security container is protected by IDS with NSF personnel responding to the alarm arriving within 15 minutes of the alarm annunciation.

(2) In a GSA-approved security container equipped with a lock meeting FF-L-2740, provided the container is located within an area that has been determined to have security-in-depth.

(3) In an open storage area (also called a secure room) constructed per reference (c) and equipped with an IDS.

(a) The space will need security personnel responding to an alarm within 15 minutes of the alarm annunciation if the area has been determined to have security-in-depth.

(b) The space will need security personnel responding to an alarm within 5 minutes of alarm annunciation if the area has not been determined to have security-in-depth.

(4) In a vault, or GSA-approved modular vault, meeting the requirements of Federal Standard 832, Construction Methods and Materials for Vaults, September 1, 2002.

b. Secret information will be stored by one of the following methods:

(1) In the same manner as prescribed for Top Secret information.

(2) In a GSA-approved security container or vault built to FED-STD 832 specifications, without supplementary controls.

(3) In an open storage area meeting the requirements of reference (c), provided the senior agency official determines in writing that security-in-depth exists, and one of the following supplemental controls is utilized.

(a) An employee cleared to at least the Secret level will inspect the open storage area once every 4 hours.

(b) An IDS meeting the requirements of reference (c) with NSF personnel responding to the alarm arriving within 30 minutes of the alarm annunciation.

c. Confidential information will be stored in the same manner as prescribed for Top Secret or Secret information except that supplemental controls are not required.

Chapter 4

MATERIAL CONTROL MEASURES

1. General. This chapter provides security policy for safeguarding controlled inventory items, including drugs, drug abuse items, and precious metals. Admission of new materials or supplies will be inventoried immediately and secured appropriately. Inventory records or databases will be updated immediately to ensure the integrity of the inventory systems in use. Each delivery will be thoroughly inspected to ensure no loss or sabotage. No personal deliveries of supplies will be allowed in restricted areas.
2. Definitions. The following definitions describe sensitive items:
  - a. Selected sensitive inventory items. Those items security-coded “Q” or “R” in the Defense Integrated Data System that are controlled substances, drug abuse items, or precious metals.
  - b. Code “Q” items. Drugs or other controlled substances designated as Schedule III, IV, or V items, per Title 21 Code of Federal Regulations 1308 (21 CFR 1308).
  - c. Code “R” items. Precious metals and drugs or other controlled substances designated as Schedule I or II items per 21 CFR 1308.
  - d. Precious metals. Refined silver, gold, platinum, palladium, iridium, rhodium, osmium, and ruthenium in bar, ingot, granule, liquid, sponge, or wire form.
3. Policy. Controlled inventory items will have characteristics so that they can be identified, accounted for, secured, or segregated to ensure their protection and integrity. Special attention will be paid to the safeguarding of inventory items by judiciously implementing and monitoring PS measures. This will include analysis of loss rates through inventories, reports of surveys, and criminal incident reports to establish whether repetitive losses indicate criminal or negligent activity. Any loss that is deemed as theft or pilferage will be reported to FLEACT Yokosuka Security for investigation regardless of the owning command.
4. Responsibilities. The Installation Commander and Commanding Officers of tenant activities will:
  - a. Establish physical security measures to protect inventory items and reduce the incentive and opportunity for theft.
  - b. Monitor the effective implementation of security requirements through scheduled inspections and staff oversight visits to affected activities.
  - c. Ensure that adequate safety and health considerations are incorporated into the construction of a security area for controlled inventory items.

d. Ensure that storage facilities and procedures for operation adequately safeguard controlled inventory items.

5. Controlled Substances Inventory. All incoming materials will be inventoried at delivery to ensure the Bill of Laden or packaging slips are accurate. If the Bill of Laden or packaging slips are not accurate, it will be reported to the appropriate responsible authority. Accountability and inventory of controlled substances will be as prescribed in NAVMEDCOMINST 6710.9, Guidelines for Controlled Substances Inventory.

6. Security Requirements for "R"-Coded Items at Base and Installation Supply Level or Higher.

a. Storage in vaults or strong rooms, as defined in SECNAVINST 5510.36B, Department of the Navy (DON) Information Security Program Instruction, or 750-pound or heavier GSA-approved security containers. Smaller GSA-approved security containers are authorized but must be securely anchored to the floor or wall. All security containers will be secured with built-in group one combination locks. Alternatively, they may be stored using any means that provide a degree of security equivalent to any of the preceding.

b. Storage areas or containers should be protected with installed IDS.

7. Security Requirements for "Q"-Coded Items at Base and Installation Supply Level or Higher.

a. The preferred storage for sensitive inventory items coded "Q" is in vaults or strong rooms.

b. Small quantities may be stored in security containers or other means approved for items coded "R."

8. Security Requirements for "R"- and "Q"-Coded Items Below Base and Installation Level (i.e., Small Unit/Individual Supplies).

a. Storage as described in paragraphs 7 and 8.

b. As an alternative, small stocks may be stored in a 750-pound or heavier GSA-approved security container. Smaller GSA-approved security containers are authorized but must be securely anchored to the floor or wall. Also, any means that provides a degree of security equivalent to any of the preceding may be used. Security containers should also be located within a continuously manned space or be checked by a security force member and/or an employee at least twice per 8-hour shift, barring any reason for the contrary.

9. Outgoing Materials and Supplies. All materials or supplies leaving the controlled environment for transfer to another area or being issues or consumed will be properly

documented using local procedures. Records will include at a minimum the material or supplies, quantity, issuing personnel, receiving personnel and reason for the transfer. Inventory records or databases will be updated immediately to ensure the integrity of the inventory systems in use.

## Chapter 5

### PROTECTIVE BARRIERS, FENCES AND SIGNS

1. Protective Barriers. The purpose of physical barriers are to control, deny, impede, delay and discourage access to restricted and non-restricted areas by unauthorized persons.

a. Active barriers consist of barrier systems that are electric, hydraulic or mechanical in nature. Examples are electromechanical drop arms, final denial barriers, sliding gates, etc.

(1) At a minimum All active barriers will be inspected weekly, and operationally tested daily.

(a) Operational tests are designed to ensure the systems are properly working.

(b) Inspections are conducted to find potential imminent mechanical failures, fluid leaks, inoperable light bulbs, debris and any other degrading factors that can be corrected before the barriers fail or to correct safety concerns.

(2) All FLEACT Yokosuka active barriers are tested and inspected daily by the Operations Division.

(3) All barrier tests and inspections will be documented on the FLEACT Yokosuka Security Facility Check Sheets and in the Consolidated Law Enforcement Operations Center (CLEOC) Desk Journal.

(4) Any issues found must immediately be reported to the FLEACT Yokosuka Security Watch Commander, and documented as well.

b. Passive Barriers are barrier systems that do not move under their own power or mechanisms. Examples are dragon's teeth, water filled barriers, planter barriers, fence lines, hills that are not human passable, etc.

c. Barriers, whether active or passive, accomplish the following if used properly:

(1) Defining the perimeter of restricted areas.

(2) Establishing a physical and psychological deterrent to entry as well as providing notice that entry is not permitted.

(3) Optimizing use of security forces.

(4) Enhancing detection and apprehension opportunities by authorized personnel in restricted and non-restricted areas.

(5) Channeling the flow of personnel and vehicles through designated portals in a manner which permits efficient operation of the personnel identification and control system.

## 2. Port Security Barrier (PSB)

a. FLEACT Yokosuka uses a PSB to enclose all piers from Berth 8 to Berth 13, which should remain closed when no vessels are scheduled to enter or depart.

b. FLEACT Yokosuka Port Operations is responsible for the operation of the PSB. Port Operations will keep the PSB closed, to the maximum extent possible. It will only be opened to meet the requirements for the Atomic Energy Bureau and for mission requirements.

c. See reference (u) for further details regarding the PSB.

## 3. Fences

a. All fences onboard Main Base, Ikego Housing Facility, Urago, Hakozaiki/Azuma Island, Tsurumi OU-1 and OU-2, Nagai, and Negishi will be constructed to meet requirements outlined in reference (g).

b. The fences will be properly posted with restricted area signs.

c. Clear zones will be maintained if possible as outlined in reference (l).

d. No signs, material, fabric, advertisements, ornamental features, equipment, etc. will be hung, tied, bolted or woven into security fencing unless it is required notices and/or signage.

e. No bicycles or wheeled personal devices will be parked along or chained to security fences.

## 4. Walls

a. Walls may be used as barriers in lieu of fences. The protection afforded by walls will be equivalent to that provided by chain link fencing.

b. Walls, floors, and roofs of buildings may also serve as perimeter barriers and signs must be posted at these areas.

## 5. Security Lattice

a. Security lattice (screens and bars) may be required in some applications to protect restricted areas, high value assets or on facilities in remote areas of the installation. See reference (l) for further guidance.



b. Openings of 96 square inches or more with the least dimension greater than six inches will be equipped with one of the following:

(1) Three eight-inch or larger hardened steel bars provided the vertical bars are not more than four inches apart with horizontal bars welded to the vertical bars at all areas where vertical and horizontal bars meet so that the openings do not exceed 32 square inches.

(2) 18-gauge high carbon manganese steel mesh with 2-inch diamond grid. 16-gauge steel mesh with 2-inch diamond grid may be used if 18-gauge is not available.

c. The bars or steel mesh will be securely embedded in the structure of the building or welded to a steel frame securely attached to the wall with hardened fastenings inaccessible from the exterior of the facility. If bolt heads can be accessed from the exterior of the facility, spot weld the bolt heads to the security screen frame to prevent easy removal.

#### 6. True Wall Requirements

a. True wall requirements are mandated for arms rooms and secured rooms.

b. True wall construction means there are no false walls or gaps between the concrete floor, walls or roof and it is all made of appropriate concrete construction creating a boxed in room.

(1) When extending walls to the base of the roof line to meet hardening of the walls for restricted areas or to protect mission critical assets use 18-gauge high carbon manganese steel mesh with 2-inch diamond grid.

(2) 16-gauge steel mesh with 2-inch diamond grid may be used if 18-gauge is not available.

7. Identification. The installation will be properly identified as a U.S. Navy Installation and government property. Appropriate signage in both English and Japanese will be used and visible from the uncontrolled side of the perimeter.

a. A blue line will be painted on the roadway leading up to entry control points. This line will be painted on U.S. government property.

b. Standardized blue lines will be maintained in a fashion that upholds the utmost professionalism. Blue lines do not serve as a point for inducing any standing use of force measures or standing rules of engagement, the official property line, or a jurisdictional boundary. The blue line should be painted prior to the entry control point on U.S. government property.

c. The blue line will be two feet in width with white lettering "U.S. GOVERNMENT PROPERTY" in English and Japanese, painted on all roadways at all entry control points.

8. Signs and Posting of Boundaries. FLEACT Yokosuka, or the tenant activity, will post appropriate signs at all Entry Control Points (ECPs), Restricted Areas and along perimeter fence lines. Signs will be a white background with red lettering for the word “WARNING”, in both English and Japanese. The rest of the sign will be black lettering for all text, and will also be in English and Japanese.

a. The following are requirements based on locations:

(1) All ECPs at Navy installations, satellite facilities, and restricted areas will be posted at regularly used points of entry with signs that read as follows:

**WARNING**  
RESTRICTED AREA—KEEP OUT  
AUTHORIZED PERSONNEL ONLY  
AUTHORIZED ENTRY INTO THIS RESTRICTED AREA CONSTITUTES CONSENT  
TO SEARCH OF PERSONNEL AND THE PROPERTY UNDER THEIR CONTROL  
INTERNAL SECURITY ACT OF 1950 SECTION 21, 50 USC 797

(2) Perimeter boundaries of restricted areas that are composed of barriers such as fences or walls not closed off by a roof or ceiling, or entry doors to storage areas for AA&E will be posted at intervals with signs that read as follows:

**WARNING**  
RESTRICTED AREA  
KEEP OUT  
Authorized Personnel Only

(3) For areas not restricted but controlled, a white sign with black lettering will be used for perimeter boundary sign and read as follows:

U.S. GOVERNMENT PROPERTY  
NO TRESPASSING

b. There is no requirement for the placement of signs however, signage will be clearly visible to personnel approaching the installation or restricted area..

(1) The interval between signs posted along restricted areas will not exceed 100 feet; non-restricted area perimeter signs will not exceed 200 feet.

(2) All barrier signs should be placed so as not to obscure the necessary lines of vision for NSF.

c. Signage will not state if the area is a Level 1, 2 or 3 Restricted Area.

9. Clear Zones

a. Unobstructed areas or clear zones will be maintained on both sides of the restricted area fenceline where possible.

(1) An inside clear zone will, if possible, be at least 30 feet. Where possible, a larger clear zone should be provided to preclude or minimize damage from incendiaries or bombs.

(2) The outside clear zone will, if possible, be 20 feet or greater between the perimeter barrier and any exterior structures or obstruction to visibility.

b. Where exterior walls of buildings form part of a restricted area's barriers, an unobstructed area or clear zone will be maintained on the exterior side of the building wall.

c. Vegetation or topographical features that must be retained in clear zones for erosion control or for legal reasons will be trimmed or pruned to eliminate concealment of a person lying prone on the ground.

(1) The vegetation should not be more than 8 inches in height and should be checked at irregular intervals.

(2) If vegetation grows in excess of allowed height the activity responsible for the restricted area will submit a Trouble Ticket to the Public Works Trouble Desk, DSN 115, to coordinate landscaping services.

d. Obstacles may exist within exterior and interior clear zones if they offer no aid to circumvention of the perimeter barrier and do not provide concealment (or provide a plausible reason to appear innocently loitering) to an intruder.

e. Alternatives to extending the clear zone where fences already exist may include increasing the height of the perimeter fence, extending outriggers, or installing double outriggers.

## Chapter 6

### INSTALLATION ENTRY CONTROL POINTS

1. General. Main Base, Ikego Housing Facility, Urago, Hakozaiki/Azuma Island, Tsurumi OU-1 and OU-2, Nagai, and Negishi have multiple ECPs that are manned by the NSF and Civil Guard Force (CGF). These facilities should be protected by a mixture of Closed Circuit Television (CCTV), guard shacks, armed sentries, security lighting, passive and active barriers, to include Final Denial Barriers.

a. ECP hours of operations may be modified or closed at any time for security or safety purposes.

(1) The Installation Commander will approve all gate closures.

(2) Any NSF member on duty may, if following established Post Orders or PPRs signed by the Installation Commander, secure an ECP if deemed necessary.

(3) All deviations from established operating hours must be reported to the Installation Commander via the FLEACT Yokosuka Security chain of command.

b. Refer to the FLEACT Yokosuka Security SOPs, Post Orders and PPRs for further information.

#### 2. Entry Control Points onboard Main Base

a. Carney Gate is located on King Street and is the main ECP. It is located on the southwestern perimeter in Base Maps grid J02 and J03. There are three inbound vehicle lanes and three pedestrian lanes. The number of lanes open varies based on traffic flow and time of day. Carney Gate can be secured by closing the pedestrian and vehicle gates and using low security padlocks already at the ECP to lock the gates.

b. Womble Gate is located on Nimitz Boulevard and is the secondary ECP and the Commercial Vehicle Inspection Area. It is located on the south-eastern perimeter in Base Maps grid M04. There are two inbound vehicle lanes and one pedestrian lane. The number of lanes open varies based on traffic flow and time of day. Womble Gate can be secured by closing the pedestrian and vehicle gates and using low security padlocks already at the ECP to lock the gates.

c. VERNY Gate is located near Building 1997 and is a pedestrian-only ECP. It is located on the western perimeter in Base Maps grid G04. There is one pedestrian lane. VERNY Gate can be secured by closing the pedestrian gate and using low security padlocks already at the ECP to lock the gate.

d. Mikasa Gate is located near Building 1400 and is a special event pedestrian-only ECP. It is located on the western perimeter in Base Maps grid P07. Mikasa Gate can be secured by closing the pedestrian gate and using low security padlocks already at the ECP to lock the gate.

3. ECP onboard Ikego Housing Facility

a. Ikego Main Gate is located near the Joint Use Baseball Field located on the Southernmost point of the perimeter in Base Maps grid M08 and N08. There are two vehicle lanes and one pedestrian lanes. The number of lanes open varies based on traffic flow and normally only one vehicle lane is open. Ikego Main Gate can be secured by closing the electromechanical sliding gates and using low security padlocks already at the ECP to lock the gates.

b. Jimmuji Gate is located near Jimmuji Train Station and is a pedestrian-only ECP. It is located on the south-western perimeter in Base Maps grid P11. Jimmuji Gate can be secured by closing the pedestrian gate and using low security padlocks already at the ECP to lock the gate.

4. ECP onboard Hakozaki and Azuma Island. Hakozaki Gate is located on the south-western perimeter and is the main ECP. It is located on in Base Maps grid E02. There is one vehicle lane and one pedestrian lane. Hakozaki Gate can be secured by closing the vehicle gates and using low security padlocks already at the ECP to lock the gates.

5. ECP onboard Tsurumi OU-1 and OU-2

a. Tsurumi is two geographically separated facilities that operate as one compound, and are codependent.

b. Tsurumi OU-1 is the southernmost facility, and the gate is located on the eastern perimeter fence line along Anzen Street in Base Maps grid F06. There is one vehicle lane and one pedestrian lane. The ECP can be secured by closing the vehicle gates and using low security padlocks already at the ECP to lock the gate.

c. Tsurumi OU-2 is the northernmost facility, and the gate is located on the western perimeter fence line along Anzen Street in Base Maps grid C11 and C12. There is one vehicle lane and one pedestrian lane. The ECP can be secured by closing the vehicle gates and using low security padlocks already at the ECP to lock the gate.

6. ECP onboard Urago

a. Urago Gate is located near Fukaura Bay and is the only ECP. It is located on the north-eastern corner perimeter in Base Maps grid F07. There is one vehicle lanes and one pedestrian lane. Urago Gate can be secured by closing the electromechanical sliding vehicle gate and using low security padlocks already at the ECP to lock the gates.

7. Policy on Searching Military and Privately Owned Vehicles at the ECP. The Installation Commander has the authority to inspect vehicles entering or departing any FLEACT Yokosuka installations for stolen government property or other contraband. The following procedures will be used whenever a vehicle inspection is conducted:

a. The inspection will be authorized in writing by the Installation Commander.

b. FLEACT Yokosuka Security personnel will be present and in charge of inspections conducted onboard FLEACT Yokosuka and follow established Standard Operating Procedures.

8. Actual or Attempted Unauthorized Access

a. The minimum amount of force necessary will be used to prevent unauthorized access to FLEACT Yokosuka and all satellite facilities. To prevent unauthorized access, NSF will attempt to utilize physical barriers (both fixed and rapidly deployable) rather than physical force (in particular deadly force).

b. Actual and attempted unauthorized access events, on foot, in a vehicle or found after the fact will be submitted in the CNIC G2 portal based on the initial information sent to the CNIC Battle Watch. CNIC N34 will create the initial unauthorized access event within the CNIC G2 portal and send the incident identification number to Commander, Navy Region Japan (CNRJ) N34.

c. The SO will complete the unauthorized access event within the G2 portal within five working days at: <https://g2.cnic.navy.mil/ca/N3/UA/SitePages/Home.aspx>.

d. Actual unauthorized access events require a Root Cause Analysis document, which is to be uploaded in the CNIC G2 portal under the unauthorized access event, and will include any additional unclassified briefs from the incident. Actual events require Installation Commander and CNRJ comments.

e. Attempted unauthorized access events do not require a root cause analysis.

(1) Attempted events do not require Installation Commander or CNRJ comments.

(2) Attempted events will also be assigned an unauthorized access identification number by CNIC N34, who will coordinate with the CNRJ N34 for any additional information.

f. See CNIC WASHINGTON DC 181832Z Apr 18, Navy Installation Unauthorized Access Root Cause Analysis Reporting for further information on reporting Navy installation unauthorized access root cause analysis.

## Chapter 7

### PROTECTIVE LIGHTING SYSTEMS

1. Protective Lighting System. Protective lighting is a psychological deterrent and visual tool employed by station security elements as an added layer of defense. This type of lighting is designed to aid the NSF in detecting intrusion, deter criminal and terrorist threats, and monitoring secured areas while maintaining adequate concealment. All security lighting will be engineered to UFC 3-530-01 standards.

a. Protective Lighting should be installed with the aid of the following guidelines:

(1) Provide adequate illumination or compensating measures to discourage or detect attempts to enter restricted areas and to reveal the presence of unauthorized persons within such areas.

(2) Avoid glare which handicaps security force personnel or is objectionable to air, rail, highway, or navigable water traffic or occupants of adjacent properties.

(3) Locate light sources so that illumination is directed toward likely avenues of approach and provides relative darkness for patrol roads, paths, and posts.

(4) Design the system to provide overlapping light distribution.

(5) Considerations should be given to future requirements of CCTV and recognition factors involved in the selection of the type of lighting to be installed.

(6) Illuminate shadowed areas caused by structures within or adjacent to restricted areas.

(7) When considering the above, do not overlook possible applications of on demand infrared lighting.

b. The following areas onboard FLEACT Yokosuka will be considered in the planning and implementation of protective lighting:

(1) Fence lines incapable of being patrolled, water boundaries, and similar areas are not required to be illuminated. Where these areas are patrolled, sufficient illumination will be provided to assist the NSF in detecting intrusion.

(2) Vehicular and pedestrian gates used for routine ingress and egress will be sufficiently illuminated to facilitate personnel safety, identification, and access control.

(3) Exterior building doors will be provided with lighting to enable the NSF to observe an intruder seeking access.

(4) Shipyards, controlled industrial areas, docks, petroleum storage areas, and other mission critical areas should be provided with sufficient illumination for the NSF to detect, observe, and apprehend intruders.

2. Technical Aspects. Environmental factors and building construction can enhance or degrade protective lighting. These factors, and selecting the appropriate lighting device, are critical in ensuring an effective illumination arc. For protective lighting consider the following:

a. The difference in building arrangements, terrain, atmospheric conditions, and other factors necessitate the design of each protective lighting system to meet the conditions peculiar to each facility.

b. Designs for protective illumination must not be curtailed below the minimum required for security. Lack of illumination contributes to increases in loss and vandalism that can more than offset energy costs. Concentrate on reducing the amount of energy used to deliver the illumination required by taking advantage of all Lighting Energy Conservation Opportunities (LECO).

(1) Evaluate LECO in terms of existing systems in the area and future requirements.

(2) Evaluate new system interactions with existing systems in adjacent areas to determine impact (other light levels, electrical transmission systems, heating and cooling systems, etc.).

(3) Wiring System should include multiple circuits in protective lighting systems. The circuits should be so arranged that the failure of any one lamp would not darken a long section of a critical or vulnerable area. The protective lighting system will be independent of other lighting systems, and be protected so that a fire or disaster will not interrupt the entire system.

3. Protection of Controls and Switches

a. Controls and switches for protective lighting systems will be inside the protected area and locked or guarded at all times.

b. High impact plastic shields may be installed over lights to prevent destruction.

4. Other Lighting Systems in Use

a. There are, other than protective lighting for security areas listed above, continuous fixed incandescent and vapor-type flood and glare luminaries on the perimeter (mounted on buildings, poles secured to buildings, and on poles).

b. Lights are utilized for security and safety, illumination for workers entering and departing during hours of darkness, and for security of supplies and equipment stored on the outside.



5. Inspection and Maintenance Responsibilities. The proper maintenance of the lighting system is paramount for continuing a quality protective lighting program. Responsibilities for the inspection and maintenance of the lighting systems are as follows:

a. Building Managers, CDOs, or Duty Watches:

(1) Conduct inspections of all protective lighting to ensure all light fixtures are operational at Entry Control Points, building exterior lighting and restricted areas under their control.

(2) Lighting inspection requirements will be codified in writing by each tenant activity.

(3) For FLEACT Yokosuka departments, all lighting will be inspected on a weekly basis.

(4) Any deficiencies or burned out lighting will be documented and a Trouble Ticket submitted for repair.

(5) Trouble Tickets will remain with the person in charge, (i.e. Building Manager, Duty Watch, etc.) of the affected area until the lighting is repaired.

b. FLEACT Yokosuka Public Works Department. Ensure that all reports of inoperative protective lights are given immediate attention and that corrective actions are taken.

6. Commercial and/or Alternate (Emergency) Power Failure

a. In the event of a commercial power failure, Public Works will be notified.

b. Public Works is responsible for the maintenance of permanently installed generators and infrastructure.

c. Alternate power source (emergency generators) should be built into existing security lighting so the loss of commercial power will not degrade security lighting.

d. In the event of a degradation of security lighting due to a loss of commercial power, portable lighting systems will be provided by Public Works until the commercial power is repaired. The order of priority will be the same as outlined in Chapter 1 Area Security, Paragraph 3 Priority of Response.

e. In the event of an alternate (emergency) power failure, Public Works will provide portable lighting systems until the power is restored.

f. Assets that are designated as critical will be provided with portable lighting systems in a cascading manner, i.e. flowing from highest priority to lowest priority. Assets will be provided portable lighting systems based on their importance to the defense of the United States of America first and work their way downward to the local level. Assets will be prioritized in the

following order: Level 3 Restricted Areas that are Assets Vital to National Security, Critical Infrastructure, Inherently Dangerous Property, and then all other Level 3 Restricted Areas. Level 2 Restricted Areas that are Assets Vital to National Security, Critical Infrastructure, Inherently Dangerous Property, and then all other Level 2 Restricted Areas. Level 1 Restricted Areas that are Assets Vital to National Security, Critical Infrastructure, Inherently Dangerous Property, and then all other Level 1 Restricted Areas. Refer to the Installation Consolidated Restricted Area List, (enclosure (1)), for Level 1 through 3 restricted areas.

g. If the power failure, either commercial or alternate, has direct impact on a restricted area a Duty Watch from the affected command will be required to man the space or keep the restricted area under constant surveillance. Restricted areas provided with protective lighting should have an emergency power source located within the restricted area. The emergency power source should be adequate within funding constraints to sustain security lighting and communications requirements and other essential services required within restricted areas.

h. Battery powered lights and essential communications should be available at all times at key locations within the Restricted Areas in the event of complete failure of primary and emergency sources of power. Public Works will test emergency power systems at designated intervals and the results will be recorded/logged and kept on file by Public Works and the restricted area Building Managers.

7. Emergency Lighting System. Emergency lighting (stationary or portable) consists of manually operated searchlights that may be lit during hours of darkness or as needed. This system is normally used to supplement continuous or standby lighting or in the event of a loss of power to supplement security lighting requirements.

a. Stationary lighting are lighting systems that are permanent and built into existing areas to allow a means of emergency lighting in the event of a loss of power or security alerts to provide greater illumination for responders. Examples are solar charged lights, light systems on independent power sources, flood lighting or area lighting.

b. Portable lighting are lighting systems that allow a means of emergency lighting in the event of a loss of power or security alerts to provide greater illumination for responders. Examples are generator powered light masts that can be located and operate independent of any power sources, battery or generator operated flood lights or area illuminating work lights that do not require commercial power.

## Chapter 8

### ELECTRONIC SECURITY SYSTEMS (ESS)

1. General. This chapter establishes minimum requirements for ESS to include but not limited to Intrusion Detection Systems (IDS) and Closed Circuit Television (CCTV), used onboard Main Base, Ikego Housing Facility, Urago, Hakozaki/Azuma Island, Tsurumi OU-1 and OU-2, Nagai, and Negishi

a. All ESS will be built per reference (f).

b. Any components or systems not within standards will not be approved for installation, unless a waiver from the Chief of Naval Operations has been approved.

c. An Authority to Operate (ATO) will be approved prior to installation of any ESS if applicable.

d. It is the responsibility of all end users to ensure their ESS are covered under a sustainment contract.

### 2. Intrusion Detection Systems (IDS)

a. IDS provides an electronic means of accomplishing area intrusion detection, alarm reporting and display, remote alarm assessment, and alerts the FLEACT Yokosuka Security personnel to intrusions in order to enhance the protection of assets and facilities.

b. IDS are designed to detect, not prevent, intrusion into a protected area and alert NSF of the intrusion.

c. IDS systems are not a barrier but add a layer of defense in the protective posture of the asset being protected. Users of IDS and FLEACT Yokosuka Security personnel will augment these systems.

d. These requirements do not supersede or override requirements of references (b), (c), (f), (j) or (k) concerning the storage of classified material, weapons, or other sensitive items.

e. All IDS used onboard Main Base, Ikego Housing Facility, Urago, Hakozaki/Azuma Island, Tsurumi OU-1 and OU-2, Nagai, and Negishi will meet the standards of this instruction.

### 3. Responsibilities for IDS

a. FLEACT Yokosuka Security Department:

(1) Responsible for responding to all alarms onboard Main Base, Ikego Housing Facility, Urago, Hakozaki/Azuma Island, Tsurumi OU-1 and OU-2, Nagai, and Negishi

(2) Responsible for monitoring all alarms that relay to the monitoring station at the Security Operations Center (SOC) located in Building 1971, Military Police Headquarters.

(3) The duty Watch Commander will ensure the oncoming Watch Commander and the PSO is briefed during shift changes concerning any alarm status issues.

b. CNRJ Regional Dispatch Center (RDC):

(1) Responsible for monitoring all alarms that relay to the monitoring station at building 3816, CNRJ Fire Department/RDC.

(2) The monitor station will be supervised continuously by U.S. citizens who have been subjected to a trustworthiness determination according to DoD 5200.2-R Personnel Security Program.

(3) RDC utilizes local nationals to monitor IDS systems but augments with U.S. Government Employees (GS) or active duty military.

c. FLEACT Yokosuka Public Works Department:

(1) Responsible for coordinating all installation and maintenance contracts with tenant activities and FLEACT Yokosuka Security Department.

(2) Minor discrepancies in existing IDS will be financed by the owning activity.

4. Prior Installed Equipment. All grandfathered units with IDS which do not meet minimum standards are not required to request waivers or exceptions.

5. IDS Waivers/Exceptions. All other requests for waivers/exceptions must be forwarded to CNRJ via FLEACT Yokosuka Security Department for comments and coordination.

6. Types of IDS Alarm Activations

a. Nuisance Alarm. An alarm resulting from the detection of an appropriate alarm stimulus, or failure to use established entry control procedures, but which does not represent an attempt to intrude into the protected area.

(1) Examples of nuisance alarms:

(a) Animal activation of detection systems.

(b) Wing-generated alarm of a fence monitoring system caused by flexing of the fence.

(2) Numerous nuisance alarms can cause complacency.

(3) All alarms will be investigated and the results documented in the CLEOC Desk Journal.

(4) The maintenance program for the IDS will ensure that incidents of nuisance alarms will not exceed one in a period of 30 days per zone.

(5) IDS alarm maintenance is not required to be conducted on every nuisance alarm, only when two are received in a 30 day period on same zone or sensor.

b. False Alarm. An alarm when there is no alarm stimulus.

(1) The maintenance program for the IDS will ensure that incidents of false alarms will not exceed one in a period of 30 days per zone.

(2) The Command Representative is responsible for contacting the IDS alarm maintenance contractor.

c. Alarm Sensor Failure (Malfunction). A malfunctioning alarm is one that the cause for the alarm has been determined but the alarm subsystem component will not reset or the system will not arm. IDS alarm maintenance will be notified immediately for malfunctioning alarm sensors.

d. Actual Alarm Activation. When a sensor detects an event prompting the system to report an alarm activation based on the sensors data.

(1) If not one of the two alarm activations above this would constitute an actual alarm activation that the IDS is designed to detect.

(2) These include accidental activations when an authorized user makes a mistake or fails to deactivate the alarm properly or if an unauthorized person makes entry without deactivating the system.

(3) Accidental alarms are not nuisance alarms and validate the system operates as designed.

## 7. Alarmed Facilities

a. Custodians of alarmed facilities will provide continuous surveillance over protected assets until the IDS system is fully functional.

b. The command responsible for the alarm must take all necessary actions to safeguard their assets during a period of IDS unreliability or failure. Refer to the appropriate guidance in reference (c) for Classified Material storage areas or reference (j) for AA&E storage areas.

c. AA&E facilities will provide personnel to maintain continuous surveillance of protected assets until the IDS system is fully functional or the assets are relocated to another approved storage facility. A means of contacting a response force is required such as a phone or radio.

d. NEX, private banking and credit union facilities have the following special guidelines:

(1) The custodian will attempt to reset the system. If unsuccessful, they will secure the facility. These facilities are not required to post guards or maintain a presence until the alarm system is restored, but are responsible for the assets they contain. Therefore, posting an employee of the facility will be at the discretion of the facility custodian.

(2) FLEACT Yokosuka Security Department personnel will not be used to guard these facilities.

## 8. IDS Failures and Mandatory Minimum Mitigation Measures

a. Catastrophic Failure. Is when the entire system or a major portion of it is inoperative.

(1) Commands responsible for the alarms space must immediately report with a duty watch to the affected areas and begin troubleshooting or initiating repairs through contractors.

(2) If the space contains top secret information and the IDS is inoperable an employee with a secret clearance will inspect the security container or space every two hours.

(3) If the space contains Secret information and the IDS is inoperable an employee will inspect the security container or space every four hours.

(4) For spaces containing Confidential information no IDS is required.

b. Major Failure. A failure in the IDS system that would allow an intruder to penetrate a restricted area boundary without crossing at least one line of detection or an individual asset. For major failures the mitigation measures annotated in paragraph a(1) through (4) will be implemented.

c. Partial Failure. This type of failure in the IDS system would allow an intruder to cross only one line of detection at an area with two lines of detection at the boundary or a portion of the facility or individual asset. For major failures the mitigation measures annotated in paragraph a(1) through (4) will be implemented.

## 9. Installation, Monitoring and Maintenance

a. Due to the nature of the IDS systems protecting our Nation's interests and Assets Vital to National Security, there are restrictions on who may install or maintain IDS systems.

(1) All IDS will be installed by qualified personnel from an approved contractor.

(2) IDS installation and maintenance will be accomplished by U.S. citizens who have been subjected to a trustworthiness determination according to DoD 5200.2-R Personnel Security Program.

b. Proper maintenance of the IDS is imperative. Systems which are not properly maintained may either fail or produce a high number of false alarms which can cause an alarm to lose credibility.

#### 10. IDS Access List Procedures

a. Access lists are a list of personnel authorized to activate/deactivate the IDS systems for a specific area and will include the following information as a minimum:

- (1) Full name (Last, First M.I.)
- (2) Rate/Rank.
- (3) Social Security Number (last four digits).
- (4) Access area, times and dates.
- (5) Contact numbers during and after normal duty hours.

b. Updated access lists will be given to RDC or the appropriate alarm monitoring station quarterly or when any change to the list is made.

#### 11. IDS Testing Requirements

a. All IDS will be tested at least quarterly to ensure systems are functional. Tests should include temporary interruption of AC power to ensure AC/DC transfer and DC batteries are functional.

b. Custodian will contact the monitoring station and inform them that an alarm test will be conducted. Authentication between the monitoring station and the custodian will be conducted to ensure the individual making the request is an authorized individual and not an actual duress situation. Ensure all entrances are closed and there is no movement of personnel within the facility. Proceed to the keypad and arm the alarm system and test each sensor as described in the following, paragraphs.

c. Personnel testing alarm systems will record and maintain a log to include the date and time of the test performed and the components tested. If there is an identified vulnerability to the asset due to a failure of the IDS it will be appropriately documented and handled at the Secret level.

d. To prevent potential intruders from staging decoy alarm tests to cover an illicit entry, tenant activities will provide RDC the dates and times of scheduled tests and the full name(s) of personnel authorized to conduct tests at least 48 hours in advance.

**12. Navy Security Force (NSF) Response to IDS. Every alarm condition will be considered a detected intrusion until resolved.** All alarm announcements will trigger a NSF response.

a. Tenant Activities will not conduct unannounced alarm activations for testing purposes without coordinating with the FLEACT Yokosuka Physical Security Division. FLEACT Yokosuka Physical Security Division will provide safety measures to include Antiterrorism Training Team Members with “red hats” and a handheld radio to monitor the response and stop the drill if unsafe conditions arise.

b. The ability to respond to intrusion attempts is a major area of concern. The guard force must be familiar with all IDS locations and avenues of approach.

c. For detailed response procedures refer to CFAY SOP-017-20 Operations Division (Patrol).

d. Security Forces Response Times

(1) FLEACT Yokosuka Security personnel response times to activated alarms will not exceed time limits outlined in governing instructions based on the asset type.

(2) A 15-minute or less response time to all alarms is expected. If the area has been determined to not have security-in-depth a 5 minute response time is required.

**13. Facility Custodians Response to IDS Alarm Activations**

a. Upon contact by FLEACT Yokosuka Security personnel, facility custodians will respond within 30 minutes.

b. Facility Custodians are required to conduct a walkthrough of the facility with FLEACT Yokosuka Security personnel.

c. If tampering or theft of protected assets is noted, NSF will guard the facility until the crime scene has been processed.

d. If the alarm system cannot be reset, the owning activity will be responsible for providing 24-hour guard/supervision until the security alarm system is operational.



e. Responding custodians will be listed on the AAL for the facility if the area protected is designated a restricted area.

(1) FLEACT Yokosuka NSF personnel will verify the custodian is on the AAL.

(2) If the custodian is not on the AAL the FLEACT Yokosuka NSF personnel will contact RDC and request someone who is allowed unescorted access to respond immediately to conduct a sweep and secure the facility.

#### 14. IDS Standardization

a. IDS employed at facilities will be integrated with the existing system to ensure uniform IDS and interoperability.

b. Integration can only be declined when DoD and/or Navy directives identify IDS requirements that the installation IDS cannot support.

#### 15. IDS Support

a. Commands requesting IDS support will develop a Memorandum of Agreement (MOA) between their CO/OIC and CNRJ that outlines operational response procedures.

b. This MOA must be in place prior to the activation of the IDS.

c. The requesting command is responsible for ensuring that the MOA remains current and accurate at all times. This includes conducting an annual review of the MOA for accuracy and validity.

16. Closed Circuit Television (CCTV). CCTV is utilized to monitor and maintain a visual record of entry control points, restricted areas, and protected spaces. CCTV installation will be conducted under the following guidelines:

a. CCTV should be installed in areas supported by IDS. This will allow for the two systems to work in conjunction with each other, providing an effective security tool for the security dispatchers.

b. Prior to the installation of CCTV, a protective lighting survey should be conducted of the applicable area. This is to ensure that adequate lighting is in place to support the operation of the camera equipment.

c. All CCTV equipment monitored by FLEACT Yokosuka Security or RDC will be recorded through digital recording equipment.

## Chapter 9

### PROTECTION OF ARMS, AMMUNITION AND EXPLOSIVES (AA&E)

1. General. This chapter covers the local physical security procedures for the protection of AA&E. This instruction in conjunction with reference (i) and (j) is intended to provide adequate protection to AA&E facilities during peacetime conditions. Any security measures in excess of these basic requirements are encouraged.
2. Responsibilities. The tenant activity CO/OIC or FLEACT Yokosuka Department Head of AA&E storage facilities will:
  - a. Establish written instructions for control and operations of AA&E storage facilities and coordinate through the FLEACT Yokosuka PSO, Fire Department and Explosive Safety personnel to ensure compliance with U.S. Navy and local instructions.
  - b. Conduct initial training for procedures in external penetration, bomb threat/suspicious package and circulation control immediately upon an individual's assignment to an AA&E facility and follow-on training for all personnel at least annually. The training will be documented by written memo that indicates the date of the training and lists those who attended.
  - c. Ensure persons allowed entry into AA&E/restricted area storage facilities are strictly limited and controlled. Visitors will be limited to official business only and signed in via a Visitors Log. This document will be maintained on file for one year from the date of last entry. Destroy one year after action completed or after next inspection, whichever is later.
  - d. Secure and arm the IDS when facilities are not directly supervised by an authorized attendant. Directly supervised is interpreted to mean that the authorized attendant has a constant visual on the storage container or facility.
  - e. Maintain access to a current copy of this instruction. Electronic copies are sufficient to meet this requirement and will be available during inspections and surveys.
  - f. Coordinate all requests to establish or construct new or modify AA&E storage facilities with PSO. Once the initial survey is conducted, the department head will submit a memorandum of request for authorization to store AA&E to the Installation Commander.
  - g. Prior to any new AA&E storage areas a Physical Security Survey must be completed by the Installation Physical Security Office.
3. Designation of a Firearms Storage Facility
  - a. The Installation Commander is the approval authority for storage of AA&E.

b. All AA&E storages will be designated in writing by the Installation Commander on the Consolidated Installation Restricted Area List (enclosure 1), after the Explosive Safety Officer has approved the storage site.

c. The activity responsible for the AA&E space will maintain designation letters for the life of the AA&E facility.

d. AA&E facilities will be protected and constructed per references (i) and (j).

4. AA&E Storage Facility Construction. Protective measures and construction standards will be met for all AA&E Spaces. All AA&E spaces must be secured with a high security lock unless exempted by reference (j) with the requirements listed below:

a. Ready for Issue (RFI) arms and ammunition may be stored together for security personnel or response personnel. RFI AA&E storage areas are not required to have a high security locking device, IDS, an AIB, or meet construction standards provided the following mitigations are met:

(1) The minimum amount of weapons and ammunition necessary for the mission are stored in the RFI, and they are kept in a locked container, standard or locally-made arms rack, or area.

(2) An armed guard or watch stander, with communication equipment to summon assistance, is within sight of the storage container or area(s) at all times;

(3) The guard or watch standers' other duties, such as monitoring alarms, must not interfere with the ability to control access to the weapons;

(4) The weapons storage container or area is inventoried at each change of watch or whenever the container is opened; and

(5) Access to the area is strictly limited.

b. All issuance of weapons from a RFI will be conducted behind a locked door and through an opening not to exceed 190 square inches when open, and when not in use will be secured with material comparable to that forming the adjacent walls.

5. Ordnance Magazines Entry/Exit. Ordnance magazines Category I and II are Level Two restricted areas. All Category III and IV magazines are Level One restricted areas.

a. For detailed Entry/Exit procedures refer to Chapter 3 of this instruction.

b. Unescorted access to Category I and II AA&E storage areas is not authorized.

6. Padlocks and Combinations Locks for AA&E Vault Doors and Containers

- a. All new and existing GSA approved weapon containers and GSA approved armory vault doors constructed to accept a three-position combination lock are required to have a UL 768 Standard, Group 1 or Group 1R mechanical combination lock installed.
- b. Group 1 locks resist manual manipulation for a period of 20 man-hours.
- c. Group 1R locks meet all of the requirements of Group 1 locks and also resist radiographic (X-Ray) attacks.
- d. Contact the FLEACT Yokosuka PSO if assistance is needed for ordering information.

7. Security Checks

- a. Per reference (j), non-duty hour checks of all AA&E and alarmed facilities will be conducted by NSF personnel and recorded on the appropriate Facility Check Sheet. These records will be maintained for a minimum of three years by the FLEACT Yokosuka Physical Security Division.
- b. Tenant activities will also establish a system for the daily after-hours checks of their restricted areas, facilities, containers, and barrier or building ingress and egress points to detect any deficiencies or violations of security standards.
  - (1) These records will be maintained for a minimum of three years by the tenant activity.
  - (2) These checks will be in conjunction with FLEACT Yokosuka Security checks.
- c. Although reference (j) delineates one check per 24 hours on most AA&E spaces each Restricted Area is required to be checked every 4 hours when unmanned or every 8 hours when manned as required by reference (k), the most stringent requirement will be used to ensure compliance.
- d. FLEACT Yokosuka Security Watch Commander will immediately increase physical security measures by directing NSF to conduct more frequent security checks of any AA&E storage area during periods of special vulnerabilities.
  - (1) Periods of special vulnerability include but are not limited to civil unrest, natural and man-made disasters, emergencies, and increased criminal or terrorist threats.
  - (2) During these periods AA&E may be required to be relocated out of the affected area to an alternate storage area location. Alternate storage locations include other approved AA&E storage locations onboard Main Base, Urago, and/or vessels moored at FLEACT Yokosuka. The primary contingency plan for transfer of AA&E to an alternate area for protection against all hazard threats (typhoons, tornados, fire, threats of terrorism, etc.) is to coordinate with the

Commanding Officer, Navy Munitions Command Pacific East Asia Division Unit Yokosuka (NMCPACEAD Unit Yokosuka) located in Urago. The SO will make arrangements with NMCPACEAD Unit Yokosuka to utilize authorized NMCPACEAD Unit Yokosuka vehicles and driver to transport affected AA&E to appropriate storage location(s).

f. The owning command of the AA&E will make all requests for support to the FLEACT Yokosuka SO in any situation where additional protective measures are needed.

g. FLEACT Yokosuka Security is ultimately responsible for the protection of all AA&E onboard Main Base, Ikego Housing Facility, Urago, Hakozaki/Azuma Island, Tsurumi OU-1 and OU-2, Nagai, and Negishi

8. Unattended AA&E. FLEACT Yokosuka SO will be notified of all incidents involving unattended AA&E. FLEACT Yokosuka CID or NCIS FEFO will immediately investigate incidents of AA&E found unattended.

9. Lost, Stolen, Unaccounted for, or Recovered AA&E. Tenant Activity CO/OIC or FLEACT Yokosuka department heads of AA&E facilities will establish written procedures in their SOPs to ensure lost, stolen, unaccounted or recovered U.S. Government AA&E are reported to the FLEACT Yokosuka SO within 2 hours of suspected or actual loss or recovery.

#### 10. Annual AA&E Screening

a. Annual personnel screenings are conducted and documented per reference (j).

b. At a minimum, the SO, AA&E Accountability Officer or AA&E Officer, Explosives Safety Officer, or other designated officer or civilian will examine service records of those being screened and discuss the duties to be assigned with the person and/or the person's present supervisor.

c. Enter dates of screening, rescreening, and associated interviews in the person's personnel record and maintain for at least 2 years after termination of the person's assignment (or six months after the final interview if the person is disqualified).

d. Determination of which traits and actions are disqualifying is at the discretion of the Installation Commander, or tenant CO/OIC or CMC (contact CNO (N09N3) for guidelines).

e. Re-screen personnel annually or when circumstances indicate a review would be prudent.

f. At each screening read the following statement to the person being screened and have them sign a copy of this statement:

- "I understand that my behavior on duty as well as off duty is expected to reflect mature, stable judgment and that I may be removed from my duties involving control of arms, ammunition and explosives, or other administrative action taken, if my behavior does not reflect

high standards. I further understand that serious harm can come from my failure to properly carry out my duties. I am aware that my improper actions or failure to carry out my duties may result in criminal prosecution, fines, and imprisonment. I understand and accept the responsibility to safeguard arms, ammunition and/or explosives."

g. Civilian government or contracted employees assigned custody operating a vehicle or providing security to a vehicle transporting AA&E will at a minimum have a favorable National Agency Check (NAC) with Written Inquiries and Credit Check. NMCPACEAD Unit Yokosuka uses only military members to conduct weapons movements off installation. FLEACT Yokosuka Security Department Active Duty NSF conducts all escorts for security off installation.

h. Military and contractor personnel will have a NAC, Local Agency Check, Credit Check as set forth in reference (j), except as provided for U.S. flag carriers. Officers of U.S. flag carriers will be licensed per U.S. Coast Guard requirements.

i. Designated carrier employees providing Protective Security Service for the transportation of items classified SECRET will possess a government-issued SECRET clearance, as provided for in reference (j), and carrier-issued identification.

## 11. AA&E Inventories

a. The AA&E Accountability Officer will conduct inventories per references (j).

b. When custody of keys are transferred to a new key custodian, both out-going and incoming key custodians will perform an inventory entailing a 100 percent count of AA&E.

c. Upon a change of command or a change of the Accountability Officer a 100 percent physical inventory of all SRC I and SRC II conventional ordnance will be conducted. This inventory will be completed within 90 days of the change of command or change in Accountability Officer, regardless of the length of time since the last inventory.

d. The Installation Commander will be regularly briefed by the AA&E Accountability Officer, on all FLEACT Yokosuka AA&E inventories, the status of command compliance with accountability controls, status of command inventory versus AA&E allowance, and AA&E requisition status via NAVSUP 724 or other locally generated form. The Installation Commander will sign acknowledging, and all records will be maintained for a minimum of two years by the FLEACT Yokosuka Armory.

e. All other AA&E facilities will count and record number of weapons and ordnance on hand when entering facility/container or at least weekly, whichever comes first.

f. Banded/locked containers will utilize a numbered seal and have an established anti-pilferage seal program.

(1) Each seal will be individually inspected during inventories.

(2) If a numbered seal is used, recorded and intact upon inspection, there is no need to break the seal.

g. RFI storage areas will have a complete inventory conducted every time the RFI is opened or upon change of the Duty Armorer.

## 12. Anti-pilferage Seals Program

a. Anti-pilferage seals programs will be established where weapons are banded/locked in containers for storage or shipping or where weapons are stored in racks for long-term storage.

b. Anti-pilferage seals are not locking devices therefore when utilized they will be frequently inspected to determine if tampering has occurred.

c. The following minimum procedures will be established:

(1) Strict accountability procedures.

(2) Procedures for destruction of cut seals.

(3) Witnesses who witnessed the cutting of the seal.

(4) Storage/Issue procedures.

d. If an anti-pilferage seal has signs of tampering, is missing, has mismatched seal numbers, improperly applied seals, or the integrity of the seal is in question the seal will be opened and a full inventory of the contents will be conducted. The seal discrepancy will be reported to the appropriate authority and resealed appropriately.

## 13. AA&E Key and Lock Control

a. The Installation Commander will designate in writing a Key and Lock Custodian and Alternate Key and Lock Custodian for AA&E facilities to FLEACT Yokosuka departments.

(1) Tenant activity CO/OIC will designate in writing a Key and Lock Custodian and Alternate Key and Lock Custodian for AA&E facilities under their control.

(2) They will place a copy of the designation letter in the same area where the AA&E Keys are stored and have the letter readily available for inspections.

b. Non-FLEACT Yokosuka department head(s) of AA&E facilities will ensure development of written procedures within their instructions that encompasses security of all conventional ordnance, weapons, weapon system structures, gates, safes, vaults, magazine storage facilities etc.

c. Key custodians will not be unit armorers or other persons responsible for the AA&E storage facility.

d. The Key and Lock Custodian for AA&E may be the facility manager or any other individual that does not have direct access to the AA&E or keys and combinations to the AA&E.

e. The Key and Lock Custodian for AA&E Facilities must be a separate individual from the Key and Lock Custodian for all other facilities.

f. The procedures for key control for AA&E facilities are as follows:

(1) All keys for the AA&E facility will be inventoried by the designated Key and Lock Custodian semi-annually or upon change of Commanding Officer, Key Control Officer, AA&E Accountability Officer, Weapons Officer or AA&E Key and Lock Custodians.

(2) Per reference (j), under no circumstances will anyone outside the AA&E facility have access to keys or key storage containers to AA&E facilities.

g. The designated Key and Lock Custodian for AA&E facilities will:

(1) Maintain accountability of all keys associated with the AA&E facility.

(2) Ensure all keys pertaining to the AA&E facility, including any spare keys, are signed over using a Key Issue Record (See Chapter 12).

(3) Maintain a Key and Lock Control Log (See Chapter 12) for recording and controlling keys, locking devices, and for the recording of semiannual key inventories.

(a) Semiannual key inventories will be conducted by the Primary or Alternate Key and Lock Custodian.

(b) This form will be maintained for a period of one year after the last entry, and then disposed per reference (j).

h. Keys providing access to Category I and II AA&E will be maintained in a GSA approved Class 5 container with a built in Group 1 combination lock.



- i. Keys providing access to Category III and IV AA&E will be maintained in a container constructed as a minimum of 20-gauge steel, and equipped with a GSA approved built-in changeable three-position combination lock or a GSA approved changeable combination padlock.
- j. Personnel not associated with the AA&E facility will not have access to the key container.
- k. When facility (container) is open, padlocks will be locked to the staple or hasp to prevent their theft, loss, or substitution. At no time will the key to a key container be left in the locking device keyway.
- l. Keys to AA&E buildings, rooms, racks, containers, IDS, and ordnance storage areas, may be secured together in the same key container.
- m. AA&E keys will be maintained separately from all other keys that do not pertain to AA&E storage.
- n. AA&E keys will be accessible only to authorized personnel designated by an AAL or similar document. The AAL will be posted inside the immediate area of the security container and protected from public view.

#### 14. Combination Changes

- a. Combinations to AA&E facilities, storage containers/vaults, and key containers will be changed annually, immediately when compromised, subjected to compromise or when assigned personnel are transferred or terminated.
- b. The AA&E Key and Lock Custodian is responsible for ensuring combination changes are in compliance with this instruction, however, only personnel authorized access to AA&E will have access to combinations or keys to the AA&E facility, safes, containers, key storage areas, etc.
- c. The outgoing Key and Lock Custodian is responsible for training their replacement on procedures for changing combination locks and requirements for documenting changes on a SF-700.
- d. Department heads will ensure personnel are trained, qualified and familiar with AA&E key and lock procedures prior to assigning personnel responsibilities to AA&E facilities.

15. Firearms and FLEACT Yokosuka Facilities. Only on-duty FLEACT Yokosuka Security personnel, NCIS FEFO and other Federal Agents are authorized access into FLEACT Yokosuka facilities with a firearm with the exception of the Pre-Trial Confinement Facility where no firearms may enter.

16. Sobriety While Carrying and Handling Weapons

- a. Carrying, handling, using, or transporting firearm(s) while under the influence of intoxicants is prohibited.
- b. Personnel who are required to carry a firearm on duty or handle AA&E will not consume alcohol or other intoxicants for a period of 12 hours before their start of the workday and have no lingering effect of the intoxicants at the time of their duties.

17. Domestic Violence

a. The Gun Control Act of 1968 was amended in the year 2000 to preclude possession of firearms and ammunition by anyone convicted of an act of domestic violence. This amendment is commonly referred to as the Lautenberg Amendment.

b. The Lautenberg Amendment makes it a felony for anyone who has been convicted of a “crime of domestic violence” to ship, transport, possess or receive firearms or ammunition, and prohibits sales or other dispositions of firearms and ammunition to such individuals. Violations may result in a maximum punishment of 10 years of imprisonment and \$250,000 fine.

c. DD 2760, Qualification to Possess Firearms and Ammunition.

(1) Installation Commander and tenant activity CO/OIC will ensure all military and civilian personnel who work with or are required to qualify on a firearm, destructive device, or possess ammunition are directed to complete the DD 2760.

(2) The DD 2760 will be completed every time a military member or civilian employee is assigned to duties requiring the use of a firearm, destructive device, or ammunition. This includes when an individual has a permanent change of station, temporary duty assignment, or permanent change of assignment.

(3) All military members and civilian employees who handle firearms or ammunition will complete the DD 2760 initially upon assignment and annually thereafter or whenever a change in response on the form would result, whichever comes first.

(4) Prior to any weapon/ammunition training/certification, personnel will be required to provide a signed copy of the DD 2760 to FLEACT Yokosuka Armory.

(5) Upon completion of training/certification and access to weapons and ammunition is no longer available, the DD 2760 will be returned to the trainee.

(6) Installation Commander and tenant activity CO/OIC will establish a program to ensure military and civilian employees reporting to the department/unit/agency and required to carry or possess a weapon completes a DD 2760 and maintain it in the individual's training record at the department/OIC/agency level.

d. Per federal law as amended, personnel who acknowledge or upon discovery of an actual conviction of an act of domestic violence will not be allowed access to any firearms or ammunition.

e. Personnel who acknowledge they are currently under investigation or have a court date for an alleged act of domestic violence will not be authorized access to government owned firearms and/or ammunition until the case has been adjudicated. Once adjudicated and if the individual is convicted of the domestic violence follow the procedures outlined in this instruction for denial to weapons and ammunition.

(1) Installation Commander and tenant activity CO/OIC of AA&E facilities will ensure written procedures and the requirements as outlined in this instruction are incorporated into department SOPs.

(2) Installation Commander and tenant activity CO/OIC of AA&E facilities will ensure those under investigation of domestic violence will be placed on the Do Not Arm/Download List and have these lists posted in all AA&E spaces.

f. Installation Commander and tenant activity CO/OIC will ensure their personnel are informed initially upon assignment and annually thereafter of the Lautenberg Amendment, its consequences, and the procedures outlined in this instruction. Document by name and date the individuals that attend these annual briefings.

18. Incidents Causing Revocation for Carrying or Assigned as Custodian to AA&E Facilities. The Installation Commander, and tenant CO/OICs will ensure procedures are established in writing within their SOPs for immediate removal of personnel involved in any domestic violence or other incidents where their integrity may be questionable, i.e., initial and confirmed positive drug testing, acts of suicide, drunk on duty, etc. Tenant CO/OICs will ensure the SECO, CSO and the ESO are immediately notified of any such incidents. Upon notification, affected personnel will be denied access to alarmed AA&E facilities. Tenant CO/OICs will initially issue a verbal order to cease carrying or accessing AA&E facilities and will follow up within 24-hours with a written order. A copy of the written order will be forwarded to the SECO, CSO and the ESO.

## Chapter 10

### KEY AND LOCK CONTROL PROGRAM

1. Purpose. This chapter is to establish a Key and Lock Control Program for FLEACT Yokosuka per references (j), (k) and (o).
  - a. This policy encompasses all keys, locks, padlocks and locking devices used to meet security and loss-prevention objectives.
  - b. This covers all departments and tenant activities onboard FLEACT Yokosuka to include low security keys, high security keys and Arms, Ammunition and Explosives Keys.
2. Discussion. Reference (k) requires each command or unit to develop a strict Key and Lock Control Program to ensure compliance with security measures delineated in references (j) and (k).
3. Scope
  - a. Included in this plan are all keys, locks, padlocks and locking devices used to protect or secure restricted areas, activity perimeters, perimeter gates, security facilities, AA&E storage facilities, critical assets, classified material, sensitive materials, pilferable supplies, as well as building keys such as storage, exterior doors and internal office doors.
  - b. Approved locking devices for the protection of classified materials are specified in reference (c).
  - c. Not included in this program are keys, locks and padlocks for convenience, privacy, administrative or personal use (e.g. desk keys, personal lockers, filing cabinets that are not filing classified materials and keys protecting personal or non-government materials).
4. Responsibilities. Security is the responsibility of all personnel, including civilian employees. The following specific responsibilities are delineated:
  - a. Commanders, Commanding Officers, or Officers-in-Charge are responsible for physical security and loss prevention within their commands or units.
  - b. The FLEACT Yokosuka SO is designated in writing by the Installation Commander as a representative and is responsible for program management and general supervision of the Key Control program. This responsibility includes:
    - (1) Submitting an appointment letter designating the Key and Lock Control Officer.
    - (2) Approving or disapproving key control subsystems.

(3) Ensuring investigations are conducted on the loss, theft or damage of keys/locks within the command key and lock control system.

(4) Making provision for the inspection of locking devices during non-duty hours by FLEACT Yokosuka Security Department personnel.

c. The Key and Lock Control Officer is responsible for:

(1) Administratively supervising the Key and Lock Control Program.

(2) Establishing and supervising the Key Control Center.

(3) Inspecting key and lock control subsystems.

(4) Approving or disapproving requests for fabrication of duplicate keys.

(5) Coordinating with the SO, PSO, and a designated representative for the procurement of locking devices and hardware.

(6) Monitoring the AA&E Control Program for Main Base, Ikego Housing Facility, Urage, Hakozaiki/Azuma Island, Tsurumi OU-1 and OU-2, Nagai, and Negishi.

d. The Public Works Officer is the agent for classified security locking devices within the command and is responsible for the following:

(1) Coordinating efforts with the SO, Key and Lock Control Officer, and Installation Security Manager to ensure physical security is maintained per references (b) and (c).

(2) Maintaining a secure central key room in which duplicate keys, key blanks, padlocks (key and combination type) and key-making equipment will be stored. Access to this area must be tightly controlled. Duplicate keys will be provided protection equivalent to the area/material those keys are used to secure.

(3) Providing adequate locking devices to department and staff offices.

(4) Installing, repairing and modifying as necessary locking devices to buildings and facilities; keys, locks and padlocks for convenience, privacy or personal use are not included in this requirement.

(5) Coordinating with the Installation Security Manager to ensure all Public Works Department personnel involved with security and locking devices have a security clearance appropriate for their particular involvement and ensuring Public Works has a qualified U.S. Citizen locksmith with at a minimum a Secret clearance to provide services for high security locking devices onboard FLEACT Yokosuka, Ikego Hills Housing Facility, Urage, Hakozaiki/Azuma Island, Tsurumi OU-1 and OU-2, Nagai, and Negishi.

e. FLEACT Yokosuka department heads will:

(1) Designate Departmental Primary Key Custodians and Alternate Key Custodians in writing and provide copies of designation letters to the Key Control Officer.

(2) Assist the SO by remaining cognizant of the physical security of the spaces under their control and ensuring each Departmental Key Custodian follows the procedures of this directive.

5. Procedures

a. Key Control

(1) The Key and Lock Control Officer will be designated in writing by the Installation Commander and be responsible for all FLEACT Yokosuka departments. This is normally the SO but is not required to be.

(2) The Key and Lock Control Officer will hold a security clearance equal to the highest level of classified material held by the command.

(3) The Key and Lock Control Officer will institute a program that indicates all keys on hand, keys issued to whom, date keys were issued and returned, as well as signatures of persons drawing or returning security keys. Reference (o) will be used as a guide for establishing the program.

(4) Key Custodians must be designated in writing by the Installation Commander to assist the Key and Lock Control Officer.

(5) Access to the Key Control Locker must be controlled and the locker must be secured when not in use.

(6) Duplicate keys will be provided protection equivalent to the asset or area that the original keys are used to secure.

(7) Continuous accountability of keys is required at all times.

(8) See Chapter 12 for forms to be used for key accountability and control.

(9) Completed key control logs will be maintained in command files for a minimum of three years, with departments, and/or tenant activities.

b. Tenant activities

(1) Each tenant activity will be responsible for its internal security program. These programs will not detrimentally affect the security of any other activity or department.

(2) Installation or modification to perimeter and internal access locking devices that would be necessary to allow entry by emergency personnel, such as the CNRJ Fire Department or FLEACT Yokosuka Security Department, will be coordinated with the FLEACT Yokosuka SO.

c. Criteria for Issuing Keys

(1) Keys for security locks and padlocks will only be issued to those persons with a need for them as approved by the FLEACT Yokosuka Key and Lock Control Officer or FLEACT Yokosuka SO.

(2) Keys will neither be issued to a member on the basis of their status or rank, nor for personal convenience.

(3) Certain categories of security assets have specific rules concerning the issue and control of keys that allow access to them.

(4) The Key Control Officer is responsible for enforcing compliance with references (j), (k) and (o).

d. Lost, Misplaced or Stolen Keys

(1) In the event of lost, misplaced, or stolen keys, cylinders, or padlocks, the Key and Lock Custodian will be notified immediately and the affected cylinders, locks, and all cores to locks with missing keys will be replaced immediately upon receipt of a Lost Key Report (See Chapter 12).

(2) Results of completed Lost Key Report will be maintained on file and retained for a minimum of three years.

(3) Replacement or reserve locks, cores and keys will be secured to preclude access by unauthorized individuals.

(4) All Lost, Misplaced or Stolen keys will be reported to the Key and Lock Custodian and/or AA&E Key and Lock Custodian immediately.

(5) The entity who lost, misplaced or suspects the key was stolen will complete the Lost Key Report with the Key and Lock Custodian who will submit the Lost Key Report to the Key Control Officer.

(6) The Key Control Officer will make the determination to replace the lock, replace keys or rekey the system based on the available information and circumstances.

(7) If the key is suspected stolen and goes to a High Security Lock or Secured Space, an investigation will be initiated by appropriate investigative agencies to find the suspect and circumstances.

(8) The Key and Lock Custodian will maintain these records for 3 years.

f. Key Storage

(1) When not attended or in use, keys will be secured in standard key cabinets. Keys to the cabinets will also be controlled.

(2) Standard cabinets are not to be used for the storage of keys to sensitive or classified materials storage. Such keys are to be stored in security containers as required by applicable security regulations.

(3) Duplicate keys, key blanks, padlocks (key and combination type) and key making equipment will be stored in a central key room.

(4) Controlled keys will not be duplicated at any time for any reason nor removed from the installation without prior written consent of the FLEACT Yokosuka SO.

g. AA&E Key Control

(1) Keys to AA&E storage buildings, rooms, racks, containers and IDS will be maintained separately from other keys, and accessible only to those personnel whose official duties required access to them. A current roster of these personnel will be kept within the unit or activity. The roster will be protected from public view.

(2) When arms and ammunition are stored in the same area, keys to that storage area will be maintained together but separately from other keys that do not pertain to AA&E storage. The number of keys will be kept to the minimum number of keys and to essential personnel only. Keys will not be left unattended or unsecured at any time. The use of a master key system is prohibited for AA&E storage.

(3) When individuals, such as duty personnel, are charged with the responsibility of safeguarding or otherwise having keys immediately available, they will sign for a sealed container of keys or conduct a full inventory. When the sealed container of keys is transferred from one individual to another, the unbroken seal is evidence that the keys have not been disturbed. If the seal is found broken, an inventory of the container's contents will be conducted and reported to the appropriate Key and Lock Custodian and Key Control Officer for reseal.

6. Locks

a. Locking Devices. Approved locking devices are listed in reference (o).



b. Rotation and Maintenance

(1) Security locks, padlocks and/or lock cores will be rotated at least annually and documented for future inspections or audits.

(2) The department head or Key Control Officer will sign rotation records and records will include the locks serial number, the new locks serial number, date lock was rotated and who conducted the lock rotation.

(3) Annual scheduled rotations, testing, lubrication and inspection will be performed on all locks, with records maintained for three years.

(4) Maintenance of all locks is necessary to prevent malfunctions caused by dirt, corrosion and wear and will be conducted using the 3M Program as applicable to the lock.

(5) All maintenance, testing and lubrication will be performed using approved procedures.

c. Padlock Security. When doors, gates or other equipment that a padlock is used to secure is open or operable, the padlock will be locked onto the staple, fence, fabric or other available secure point to preclude the switching of the padlock.

d. Lockouts

(1) Lockouts occur when a locking mechanism fails to operate as designed and access is no longer possible or access becomes unreliable. In the event of a Lockout, Installation Physical Security or command Locksmith will inspect the lock to determine the cause of the Lockout, particularly to verify if the Lockout is due to mechanical failure or sabotage and/or tampering.

(a) Mechanical Failure Lockouts occur due to wear on the locking device, age, or component failures not caused by illegal activity. If a lock is becoming unreliable or signs of wear are showing it is best to replace the lock completely before a lockout occurs. Mechanical failure Lockouts will be reported to the Key Control Officer who will make a determination to replace the lock, replace keys or rekey the system based on the available information and circumstances. The Physical Security Specialist who inspected the lock will ensure a Desk Journal of all Lockouts are made in CLEOC.

(b) Sabotage or tampering, if sabotage and/or tampering is suspected an investigation will be initiated by appropriate investigative agencies to find the suspect and circumstances. Signs of sabotage or tampering include pick marks on core, visible cuts, burs or pry marks caused by force or markings on the lock displaying the combination. Once investigators clear the lock the Physical Security Specialist who inspected the lock will ensure a Desk Journal of the Lockout is made in CLEOC. If sabotage or tampering is suspected the locking systems or combinations will be changed immediately.

(2) All lockouts involving security locks will be reported to the FLEACT Yokosuka Security Department, logged into CLEOC and investigated by Physical Security Division or a command Locksmith, to determine if the failure of the locking device occurred because of a product failure or as a result of attempted or actual illegal penetration.

(3) The FLEACT Yokosuka SO will be notified of the determination, upon completion of the investigation and documentation retained on file for three years.

## 7. Inventories

### a. Controlled Keys

(1) The Key and Lock Control Officer or Key and Lock Custodians will conduct a semi-annual inventory of all keys.

(2) All keys will be inventoried upon change of department head, change of Key and Lock Control Officer, Key and Lock Custodians, or when loss of keys or loss of integrity of the Key Control program is suspected.

(3) Results of inventories will be provided in writing to the Key and Lock Control Officer. Records will be maintained for three years.

### b. AA&E Keys and Locks

(1) Inventories of AA&E keys and locks will be conducted semi-annually. Inventory records will be retained in the unit files for a minimum of three years and then disposed of per established procedures.

### c. Combinations

(1) Combinations will be changed as required or annually at a minimum. Containers storing classified material are the responsibility of the designated classified custodians in each department.

(2) SF-700s will be maintained in a separate room or container, follow SF-700 requirements outlined in reference (b) for classified combinations.

(3) Records of combination changes will be maintained in a similar fashion as Key and Lock Rotation records and maintained for three years.

(4) The combination for containers storing classified material will be marked to the equivalent markings as the material being protected, i.e. if secret documents are stored in a safe the combination to that safe will be marked and protected as "SECRET."

(5) Personally Identifiable Information is not considered classified.

8. Action

a. The FLEACT Yokosuka SO will nominate a Key and Lock Control Officer and submit an appointing letter to the Installation Commander for official designation. The FLEACT Yokosuka SO may be the Key and Lock Control Officer.

b. The Public Works Officer will maintain a secure central key room with controlled access with key manufacturing equipment and blank keys as needed.

c. FLEACT Yokosuka department heads will designate a Departmental Key Custodian in writing signed by the Installation Commander and maintain this form for future inspections.

d. Physical Security Division will inspect the tenant command's Key and Lock Control Plan for compliance with this instruction during the annual Physical Security Surveys. During these surveys it is the tenant commands responsibility to provide all documentation in an organized manner.

9. Forms. Diligent record keeping is paramount to maintaining integrity of the Key and Lock Program. The following forms will be used in maintaining a high level of control and integrity over the program while providing objective quality evidence of program compliance. All Key and Lock Control Program records will be maintained for three years.

a. Key Inventory Log (See Chapter 12): This form will be used when conducting inventories of keys located outside central key rooms which are issued to watch stations. This form will be used for semiannual inventories of sub-custody keys. An electronic inventory with the same information may be used in lieu of this form. A memorandum will be signed by the Key Custodian and forwarded to the Key Control Officer, the Key Control Officer will sign the memorandum as acknowledging the inventory was completed and acknowledging any discrepancies. The Key Custodian may request Physical Security to audit key programs with large discrepancies or deficiencies.

b. Key Control Log (See Chapter 12): This form will be used to control and maintain records of divisional keys that are used daily, but not specifically signed out to one individual. Key Control Register's should be bound to prevent loss of record. Log books will not be used to meet this requirement. This form may be used for controlled keys or AA&E keys within those programs.

c. Key Issue Record (See Chapter 12): This form will be used to issue an individual person a key for a long period of time, such as an office key or padlock key. That individual will be responsible for the key while it is issued to them.

d. Lost Key Report (See Chapter 12): The Lost Key Report will be completed immediately by the person who was assigned the key upon discovery that they have lost the key. The Lost Key Report also identifies the lost asset to the department head, and Key and Lock Custodian, resulting in the core being replaced or padlock changed. Loss of keys to AA&E or classified

material storage areas may prompt an investigation to determine if the key was stolen for illegal use. This will be the Key and Lock Officer's discretion based on the available facts and circumstances surrounding the Lost Key Report.

e. Key Manufacturing Request (See Chapter 12): This form will be used to request additional keys be made for locks or change locks. In order to create a key a sample key must be submitted with this form so the key can be duplicated. Never request a key to be duplicated if it states on the key "DO NOT DUPLICATE" or keys to High Security Locking devices. No one is authorized to use non-Navy means to duplicated keys in a Key Control Program.

f. Key Inventory Record (See Chapter 12): This form should be used while conducting the semi-annual inventories of keys. This form provides the date the key was inventoried, number of keys and who inventoried the keys. It also allows for the noting of any discrepancies. An electronic inventory with the same information may be used in lieu of this form. A memorandum will be signed by the Key Custodian and forwarded to the Key Control Officer, the Key Control Officer will sign the memorandum as acknowledging the inventory was completed and acknowledging any discrepancies. The Key Custodian may request Physical Security to audit key programs with large discrepancies or deficiencies.

Chapter 11

INSTALLATION ACCESS CONTROL POLICY

1. Purpose. To establish the security and identification requirements for installation access and to outline Defense Biometric Identification System (DBIDS) registration requirements per guidelines established in reference (n).
2. Scope. This instruction applies to all persons seeking access to all FLEACT Yokosuka to include its satellites and outlying facilities.
3. General. The Department of Defense (DoD) Common Access Card (CAC) is the principal card enabling access to buildings, facilities, installations, ships and controlled spaces. The CAC is also the primary form of identification employed for access to FLEACT Yokosuka. Personnel must have a valid purpose to be on the installation and be properly sponsored, as applicable. Possession of a valid/authorized credential does not automatically authorize access to the installation.
  - a. All personnel requesting access must provide justification/purpose for access in writing to FLEACT Yokosuka Visitor Control Center (VCC). Except as noted, all passes will be issued through DBIDS.
  - b. Access will either be unescorted, escorted, or trusted traveler when authorized. Paper passes will be issued to those requesting access for 60 days or fewer. DBIDS cards will be issued to those requiring access for 31 days or more. Personnel with 30 days or fewer, but perform work in the elements may request a DBIDS card. Access times will be 0500-2359. Only those meeting the requirements in this policy will be authorized overnight access. The only exceptions will be the situations described in section 6.
  - c. Unescorted access requires authenticating an individual's identity and determining their fitness using the following guidelines:
    - (1) Identity Proofing. The process of providing sufficient information (e.g., identity history, credentials, and documents) when attempting to establish an identity. The following credentials are identity proofed at the card issue site from federally authorized identity documents, and will be considered identity proofed. CAC, Uniformed Services Identification (ID) Card issued to military retirees and military family members, Non-DoD Federal Personal Identification Verification, United States (U.S.) Passport or Passport Card, Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa, or others listed in reference (a) and chapter 16. **(Note: While certain identification is approved for identity proofing, in order to register a visitor into DBIDS, the visitor must have an ID with an ID number associated. U.S. Citizens are required to**

**provide their Social Security Number (SSN), Certificate of Naturalization or Taxpayer ID Number to receive a DBIDS pass to access the installation.)** Personnel authorized to perform identity proofing will be designated in writing by Commander, FLEACT Yokosuka to perform these duties.

(2) Vetting. An evaluation of an applicant or card holder's character and conduct for approval, or denial of the issuance of an access control credential for physical access. The SECNAV 5512/1 is the sole means to initiate background checks on all visitors and/or contractors/vendors. Every background check for the purpose of access control requires completion of SECNAV 5512/1 for accountability purposes. All original background check documents will be maintained for three years or until the Department of Justice conducts their periodic audits, whichever is greater. All records will be maintained at the Visitor Control Center. Review of the individual's entire criminal history, not limited to a specific time frame is required for installation access per reference (a); therefore, non-U.S. citizens must additionally provide a completed Personal History Statement (USFJ Form 196aEJ/196bEJ) when requesting installation access.

(a) A background check is required for minors 10 to 18 years old to receive unescorted access. The parent or legal guardian of a minor ages 10 to 16 years old will sign the SECNAV Form 5512/1.

(b) A favorable background check is valid for 179 days. Additional requests for base access within the 179 days will not require an additional SECNAV 5512/1 or background check.

(c) After fitness determination results are returned on an individual, VCC staff will enter the date the background check was conducted and results in the DBIDS registration workstation in the remarks section.

(3) Fitness. The level of character and conduct determined necessary for the basis of access control decisions. Prior to issuing access credentials, the minimum fitness determination standard requires an inquiry of the National Crime Information Center (NCIC) Persons Files, National Law Enforcement Telecommunications System, Interstate Identification Index, NCIC National Sex Offender Registry, Terrorist Screening Database, Department of Justice National Sex Offender Public Website, Consolidated Law Enforcement Operation Center, and DBIDS for debarments. Although FLEACT Yokosuka has NCIC access, for local nationals and foreign nationals, FLEACT Yokosuka will use the United States Forces, Japan (USFJ) equivalent local authoritative data sources, including host nation law enforcement and the Personal History Statement to meet the intent of this policy as well as the SECNAV 5512/1.

d. FLEACT Yokosuka satellite compounds do not have DBIDS capabilities. Additionally, there are circumstances that will not allow a visitor to be registered into DBIDS. Refer to section 12 for contingencies for non-DBIDS utilization.

e. Escorted access is for personnel who require access without determination of fitness and must be accompanied by a sponsor with authorization to escort the individual. The sponsor

accepts responsibility for the fitness and conduct of the escorted individual and the escort requirement is mandated for the duration of the individual's visit.

f. DBIDS. All guests requesting access to FLEACT Yokosuka are required to register in DBIDS. DBIDS registration is required for vehicle passes. All vehicle passes will be issued per reference (t).

(1) Personnel requiring access for 31 days or more will be issued a DBIDS card once all required documentation is provided to the VCC and registration is completed. Visits for 30 days or less will receive a paper DBIDS pass.

(a) Short-Term Visitor Passes. Visitors who successfully complete the Visitor Control Process (VCP) with an acceptable purpose and for a duration shorter than seven days, but who are ineligible for enrollment pursuant to paragraph 0307 of reference (n), will be issued a short-term DBIDS paper pass. The pass will be valid only for the shortest duration of the time required for the visitor's established acceptable purpose. The maximum duration allowed by Commander, Navy Installations Command is seven days for short-term visitors.

(b) Long-Term Visitor Credentials. A DBIDS credential or DBIDS paper pass will be issued to individuals who successfully complete the VCP with an acceptable purpose with a duration longer than seven days and who do not possess an enrollable acceptable credential.

(2) Access to FLEACT Yokosuka is based upon careful screening criteria. All persons will be assigned an access authorization category depending upon their status. All completed personnel records registered in DBIDS will be maintained as an active record until the person(s) is expected to leave or changes employment status. All registration records will be valid for no longer than three years.

(3) In order to register a visitor into DBIDS, the visitor must have an ID with an ID number associated. Certain identification credentials are approved for identity proofing, but may not be sufficient for vetting, determination of fitness or DBIDS registration.

(a) U.S. Citizens are required to provide their SSN, Certificate of Naturalization or Taxpayer ID Number to receive a DBIDS pass to access the installation.

(b) Non-U.S. visitors to Japan with a valid passport and visa, must provide their passport for DBIDS registration and access to the installation.

(c) Japanese residents are encouraged to provide a passport. If a passport or driver's license is not available, the "My Number Card" or notification that contains the individual's "number" can be utilized. Section 23 contains samples of authorized identification cards. Resident cards can be utilized as a form of identity proofing, but additional identification is required for registration into DBIDS.

(4) DBIDS passes require a picture and fingerprints for all visitor registrations. Failure to provide either can result in denial of base access for escorted or unescorted access.

(5) Pre-Enrollment. DBIDS pre-enrollment is available at <https://dbids-usfj.dmdc.mil/portal/>. Guests may use this option to reduce waiting time at the VCC. Applicants will need to provide their information to include name, ID type and ID number (must match the ID provided to the VCC upon arrival), biographical data, contact information and sponsors information. Once complete, the guest will need to provide the VCC with the QR code or a printed copy of the completion page with the scannable bar code. The information will be available for the VCC to pull for one month.

(6) Age Limitations. Minors 12 years old and younger are not required to obtain a gate pass as long as they are immediate family members or relatives of the sponsor or are accompanied by a parent or an approved guardian.

(a) Command Sponsored Minors

1. Unescorted children transiting to and from off-base school are required to obtain a CAC (10 years and older) or DBIDS card (younger than 10 years).

2. After 2000, minors 17 years old and younger must be accompanied by a parent or guardian.

(b) Non-Command Sponsored Minors

1. After 1700, non-command sponsored minors 18 years old and younger must be accompanied by a parent or approved guardian.

2. Japanese junior high school or high school students who are 18 years old and younger must provide photo identification along with an identification number, see Figure 1 for identification samples. In order to be registered in DBIDS and provided a pass for access to the installation.

g. Liberal Guest Policy. On the third Tuesday of each month, Japanese holidays and designated special occasions, Master Labor Contract and Indirect Hire Agreement employees who possess a permanent gate pass may request entry for up to five guests from 0900 to 2000. Guests may only visit the sponsor's work site and authorized dining facilities.

h. Bazaars held by a command or an authorized organization. Requests for installation access for vendors and vehicles must be submitted to VCC two weeks prior to the event. All vendors must be escorted at all times unless requirements for unescorted access are met. All vehicles must be inspected by Military Working Dogs prior to entering the installation.

i. Media. Only personnel assigned in an official public affairs capacity are authorized to escort media on the installation.



j. Sponsor or sponsoring command

- (1) Prepares registration forms for access credential applicants/guests.
- (2) Verifies applicants/guests register their vehicle according to installation policies and procedures.
- (3) Escorts prospective contractor employees from the installation Entry Control Point to the appropriate office to initiate identity proofing and vetting for DBIDS Card issuance.
- (4) Ensures contracts contain requirements for contractor personnel to return DBIDS cards to the VCC when the contract is completed, or when a contractor employee no longer requires access to the installation.
- (5) Ensures issued access credentials are retrieved and returned to the VCC when the relationship that served as justification changes, or is terminated.
- (6) Provides the Security Officer relevant information from the Multiple Threat Alert Center.
- (7) Sponsoring commands are responsible for providing official documentation of an access requirement, mission essential and emergency essential status in order to provide the employee appropriate access permissions.
- (8) If an official visitor is already enrolled into DBIDS, sponsors may pick up a pre-printed, escort required DBIDS credential from VCC.
- (9) The following personnel are allowed to enter FLEACT Yokosuka without DBIDS registration:
  - (a) Japan Self-Defense Force members.
  - (b) Japan Maritime Self-Defense Force (JMSDF) family members who are allowed to enter the base possessing a valid JMSDF Family Member ID.
  - (c) Official visitors who have a need to conduct business or make periodic protocol visits onboard FLEACT Yokosuka who present a current ID card.
  - (d) JMSDF Contractor. Must present a JMSDF bilingual pass with an orange border to enter the installation.
    1. A background investigation will be conducted through JMSDF or other appropriate authority.

2. Commander, FLEACT Yokosuka exercises final authority over all base access.

(e) United Nations Command (Rear) personnel who possess a United Nations ID Card as shown in Section 23.

(f) U.S. Embassy personnel with valid credentials.

k. Approval and Denial Authority

(1) The FLEACT Yokosuka Security Officer is the final authority for approval or denial of requests covered by this instruction and will be delegated in a “By direction” letter.

(2) The Installation Access Request form requires endorsements prior to approval. Commands are required to endorse requests for official visitors, and for House Guest Pass requests longer than 90 days.

(3) Family Housing must endorse requests for personal guests staying in Family Housing. The relationship of the guests must be written on the request for Family Housing records. The sponsor of the guest must have this completed prior to providing the request to the VCC.

(4) Naval Criminal Investigative Service Far East Field Office (NCIS FEFO) must endorse requests for DTCNs. The VCC will route the request and all documentation to NCIS FEFO for its recommendation.

4. Forms. Forms are available for download from [https://navalforms.documentservices.dla.mil/formsDir/\\_SECNAV\\_5512\\_1\\_11787.pdf](https://navalforms.documentservices.dla.mil/formsDir/_SECNAV_5512_1_11787.pdf) and from CFAY VCC Homepage. [https://www.cnic.navy.mil/regions/cnrj/installations/cfa\\_yokosuka/om/security/industrial\\_security.html](https://www.cnic.navy.mil/regions/cnrj/installations/cfa_yokosuka/om/security/industrial_security.html). The complete list of required forms and their availability is contained in Chapter 12 of this instruction.

5. Definitions of Authorized Personnel

a. Authorized Personnel. All United States (U.S.) military personnel including members of the Japan Self-Defense Force (JSDF), U.S. military reserve, Department of Defense (DoD) U.S. civilian employees, and U.S. Navy contractors who are stationed at FLEACT Yokosuka.

b. Family Members. All command sponsored family members of U.S. military and civilian personnel. Family members of military or U.S. civilian employees and contractors not stationed at FLEACT Yokosuka are considered visitors.

c. Immediate Family Members. Family members of any sponsor or sponsor's spouse are defined as parents, children, grandparents, grandchildren, siblings and sibling's spouse and children.

d. Local Hired Employees. All Master Labor Contract (MLC); Indirect Hire Agreement (IHA), and Hourly Pay Temporary (HPT).

e. Direct Hired Employees. All Personal Service Contractors (PSC) hired directly by a specific command.

f. Domestic Help Employees. Maids/Housekeepers/Nannies hired by Status of Forces Agreement (SOFA) personnel.

g. Local Contractors. Contractor representatives authorized through the procedure described on reference (s) to conduct business within FLEACT Yokosuka.

h. Off-Base Taxi Drivers. Host nation civilian drivers who are authorized to conduct taxi services within FLEACT Yokosuka.

i. Government of Japan (GOJ) Officials. Official personnel whom require random access to FLEACT Yokosuka on a regular basis.

j. Visitors. Any person with a legitimate request or requirement for short-term access to FLEACT Yokosuka for the purpose of conducting official business or for private visits.

(1) Authorized Personnel Visitors. All military personnel, DoD U.S. civilian employees, and U.S. Navy contractor who are not permanently stationed in FLEACT Yokosuka. Japanese Defense Academy professors and cadets except personnel whose nationality is listed in reference (p); U.S. Embassy personnel; United Nations Command personnel who are not stationed in FLEACT Yokosuka; all retired U.S. military personnel; U.S. military reserve personnel and their family members when bearing bona-fide identification cards; and non-command sponsored family members.

(2) Gold Star Survivors (GSS). Will be issued a Defense Biometric Identification System (DBIDS) card once all required documentation is provided to the Visitor Control Center (VCC) and registration is completed. Fleet and Family Services Center (FFSC) has a representative for Gold Star Survivors who will sponsor personnel for base access and issuance of DBIDS card.

(a) The Navy Gold Star (NGS) Family program provides long-term casualty assistance and ensure the GSS remains connected to the Navy family for as long as they desire. GSSs are the families of Service Members who died on Active Duty, regardless of the Service affiliation or cause of death. "Family" includes: Spouse, Parents (Biological, Adoptive, Step, Foster), Siblings (Brother/Sister, Half Brother, Half Sister, Adoptive), Children (Biological,

Adoptive, Step). Survivors must be able to access Commander, Navy Installations Command (CNIC) installations for support (e.g., FFSC visits), ceremonies, and events in order to continue to be part of the Navy family. However, many do not have a DoD identification card.

1. The GSS Card, which is issued by the local NGS Coordinator, will be accepted as the purpose for requesting access.
2. The GSS will require identity proofing and fitness determination.
3. Once the GSS has met all of the installation access requirements, they will be issued a DBIDS card with an expiration date 364 days from the date of issuance.
4. The GSS will be vetted annually to renew the DBIDS card.
5. If the family member does not meet the criteria for fitness according to this manual, the installation CO may consider a waiver using the guidelines in the manual. The same process for waiver approval/denial will be followed for Gold Star family members as for any other DBIDS applicant.
6. COs will codify access control procedures for Gold Star family members in applicable access control plans.

(3) U.S. Government Officials. All personnel on temporary assignment to a specific command and employed by a U.S. Government agency to conduct business with the U.S. Government (except personnel who are nationals of a country listed in reference (p)). Designated Third Country Nationals (DTCNs) must be pre-approved by the FLEACT Yokosuka Security Officer to enter base. All personnel must have a passport and Temporary Additional Duty (TAD)/Temporary Duty (TDY) orders or an Authorization Agreement and Certification of Training (SF 182). Access to FLEACT Yokosuka, will be allowed after one of these documents have been shown to and verified by NSF at the ECP. Access will only be granted for the specific period of time indicated on the TAD/TDY orders or SF 182. Entry/Exit via Carney, Womble, and Aeon gates is authorized.

(4) Local Hired Employees (MLC/IHA). With the exception of personnel whose nationality is listed in reference (r), Local Hired Employees assigned to U.S. Forces, Japan (USFJ), but not FLEACT Yokosuka may access the installation if they are on temporary assignment to a specific command. See Multi-Installation Access for more information. Local national employees (MLC/IHA/HPT) whose nationality is listed in reference (p) must be pre-approved to enter the base by the Installation Commander or approving authority. After favorable background check has been conducted and access is approved by the Commander, the employee will be allowed to access the installation unescorted.

(5) U.S. Merchant Mariners. A Military Sealift Command (MSC) representative will provide the VCC a "Vessel Shore Party Access List" for access to FLEACT Yokosuka and all satellite areas under Commander, FLEACT Yokosuka authority with the exception of Yokohama

North Dock. The list will be limited to the names of Contract Mariners (CONMAR) who have been cleared per existing MSC policy, including El Paso Intelligence Center checks. Updates or changes to the Access list or dates of access required must be submitted by an MSC representative.

(a) Each cleared MSC CONMAR on the Shore Party Access List will possess and present their Merchant Mariner Credential, including a Transportation Worker Identification credential, for access.

(b) Entry Control Point (ECP) sentries will verify the CONMAR is on the Vessel Shore Party Access List before granting installation access.

(c) MSC Civilian Mariners carrying Common Access Cards (CACs) are authorized access.

(d) DTCNs, contractors not a part of the ship's crew, or those not meeting the clearance requirements above are required to complete an installation access request.

(6) Foreign Ships. Foreign ships (not U.S. or Japanese) berthed at FLEACT Yokosuka will be sponsored by the United Nations Command (UNC). Request for base access with the entire crew list, not including DTCNs and contractors that are not ship's crew, will be provided by a UNC representative to the VCC as soon as feasible prior to the ship's visit. Updates or changes (i.e. crew swap) will also be provided by a UNC representative. This allows the ship's crew unescorted access from the ECP to their ship. Crew members will not be authorized a vehicle pass unless a request is received by the VCC from the UNC (for official purposes only).

(7) GOJ Special Agents and Public Interest Corporation. The following GOJ representatives and members of public interest corporations who need to conduct official business or make periodic protocol visits onboard FLEACT Yokosuka are allowed to enter the base after verification of their agent ID by FLEACT Yokosuka NSF. All applicable commands must submit a sample of their current ID to the FLEACT Yokosuka Security Officer:

(a) Japanese Police. Personnel with a valid Japanese Police ID are allowed to enter the base on official duties. Any official duties that pertain to law enforcement or are investigative in nature must have approval from Commander, FLEACT Yokosuka prior to entry. Their official or approved vehicles are also allowed to enter the base. The Japanese Police officers must inform NSF/FACP personnel of their intentions and destination to be relayed to the FLEACT Yokosuka Security Officer and Command Duty Officer (CDO). In any instance, if it is determined by the FLEACT Yokosuka Security Officer that a security escort must be provided the Japanese police will wait for an escort to accompany them to their destination.

(b) Japan Coast Guard (JCG). Personnel with a valid JCG ID are allowed to enter the base as long as they are on official duties. Their official or approved vehicles are also allowed to enter the base. JCG personnel must inform NSF/FACP personnel of their intentions and destination to be relayed to FLEACT Yokosuka Security Officer and CDO. In any instance, if it

is determined by the FLEACT Yokosuka Security Officer that a security escort must be provided, the JCG will wait for an escort to accompany them to their destination.

(c) Japan Regional Defense Bureau (JRDB) personnel. JRDB personnel with a valid JRDB ID are allowed to enter the base as long as they are on official duties. Their official vehicles requested by FLEACT Yokosuka Director, Military Liaison and Civil Affairs are allowed to enter the base without obtaining a vehicle pass as long as a JRDB member is driving. Personnel with a valid Ministry of Defense ID are allowed to enter the base as long as they are on official duties.

(d) Ministry of Education, Culture, Sports, Science & Technology (MEXT). Personnel and vehicles of MEXT requested by Commander, Navy Region Japan/Commander, U.S. Naval Forces, Japan (COMNAVFORJAPAN) are allowed to enter the base with a valid MEXT ID.

(e) Japan Post (JP) Post Group. Personnel and vehicles of JP Post Group requested by Fleet Logistic Center Yokosuka are allowed to enter FLEACT Yokosuka for mail delivery purposes only. The list of personnel and vehicles must be submitted and updated whenever changes occur. Route of travel is only allowed between the Main Gate and Fleet Post Office, COMNAVFORJAPAN Legal Office (Building C-1), and FLEACT Yokosuka Office of the Staff Judge Advocate (SJA)(Building C-31).

(f) Japanese Red Cross. Personnel and vehicles of Japanese Red Cross are allowed to enter the base with a valid Japanese Red Cross ID. Prior to the vehicle's arrival, VCC/Security department must be notified of the vehicle's arrival by the appropriate authority (U.S. Naval Hospital (NAVHOSP) Yokosuka).

(8) Other SOFA Visitors. Other personnel attached to U.S. Government agencies, but who are entitled to specific medical/dental or other services onboard FLEACT Yokosuka are allowed to enter the base with a valid ID.

(9) One-day Personal Guests for JSDF Personnel. All guests must obtain a guest pass from FLEACT Yokosuka VCC prior to entry to the base. Minors 12 years old and younger are not required to obtain a gate pass as long as they are immediate family members or relatives of the sponsor or are accompanied by a parent or an approved guardian.

(10) One-day Official Guests. All official guests including local contractors must be escorted while onboard after obtaining a guest pass from FLEACT Yokosuka VCC.

## 6. Escort Privileges

- a. The following are authorized escort privileges per the chart below:

(1) **Authorized Personnel.** All U.S. military personnel including members of the U.S. military reserve, DoD U.S. civilian employees, and U.S. Navy contractors who are stationed at FLEACT Yokosuka.

(2) **Military Personnel not stationed at FLEACT Yokosuka** may escort guests. U.S. Navy contractors not stationed at FLEACT Yokosuka or with less than 90-day contracts or orders may not escort guest.

(3) **Family members.** All SOFA sponsored, accompanying family members of U.S. military personnel 18 years old and older.

(4) **Only one-day personal guests for JSDF personnel.** All guests must obtain a guest pass from FLEACT Yokosuka VCC prior to entry to the base.

b. The following personnel also have special circumstances which require escort privileges:

(1) **U.S. Government Officials.** Personnel with a CAC are authorized to sponsor personal guests onboard the installation. Those without a valid CAC will only be authorized to escort official guests.

(2) **MLC/IHA.** Do not usually have escort privileges. Those with an official requirement will have escort privileges after the department or tenant activities provides written request to the VCC. Local hire employees also may escort guests during the third Tuesday of every month per the Liberal Guest Policy.

(3) **MSC.** MSC Civilian Mariners who are CAC holders and on the Shore Party Access List are allowed to escort official guests (with proper ID) on-base. However, they are not allowed to escort any personal guests with the exception of immediate family members.

(4) **Local Contractors.** Certain contractors are representatives authorized to conduct business within FLEACT Yokosuka. Requests for contractors to be authorized escort privileges will be per reference (s) and only for official purposes their background checks must be completed.

(5) **JSDF.** All Active Duty JSDF personnel and JSDF retiree identification holders are authorized to sponsor personal guests onboard the installation. However all guests need to be enrolled onto DBIDS. JSDF retiree can't sponsor official guests.

c. The following personnel are not authorized to escort under normal circumstances:

(1) **Approved Private Organizations** themselves are not authorized to sponsor personnel. Only Authorized Personnel who are members of the private organization may sponsor and escort guests. Members and volunteers of the private organization are required to meet the escort limitation based on paygrade and as defined in the table at the end of this chapter. Personnel may use a pre-authorized request to escort a maximum of 10 personnel at one time for special

events. Private Organizations may request vehicle access for non-immediate family members only for the purpose of events. Vehicle overnight access is not authorized.

(2) Visiting Family Members. Visiting family members of any sponsor or sponsor's spouse are defined as parents, children, grandparents, grandchildren, siblings and sibling's spouse and children that are not SOFA or command sponsored.

(3) Direct Hired Employees. All personal service contractor(s) hired directly by a specific command.

(4) Domestic Help Employees. Maids/housekeepers/nannies hired by SOFA personnel.

(5) Local Contractors. Contractor; representatives authorized to conduct business within FLEACT Yokosuka.

(6) Off-Base Taxi Drivers. Host nation civilian drivers who are authorized to conduct taxi services within FLEACT Yokosuka.

(7) GOJ Officials. Official personnel whom require random access to FLEACT Yokosuka on a regular basis.

(8) Visitors. Any person with a legitimate request or requirement for short-term access to FLEACT Yokosuka for the purpose of conducting official business or for private visits.

(9) U.S. Contract Merchant Mariners. MSC Contract Mariners may not escort guests.

(10) Foreign Ships. Foreign crew members may not escort personnel to include contractors.

(11) Personnel in the U.S. Navy Delayed Enlistment Program (DEP) may not escort personnel.

(12) GOJ Special Agents and Public Interest Corporation to include JPS, JCG, JRDB personnel, MEXT and Japanese Red Cross may not escort personnel.

(13) DoD U.S. civilian employees not stationed at FLEACT Yokosuka may not escort guests. U.S. Navy contractors not stationed at FLEACT Yokosuka or with contracts shorter than 90 days or orders may not escort guest.

| Status/Grade                            | Number of Guests/vehicles              |
|---|--|
| <b>Military as defined in Section 7</b> |  |
| E-6 and senior                          | Six guests and three vehicles.         |
| E-5 and junior                          | Four guests and three vehicles.        |
| <b>JSDF Personnel and JSDF Guests</b>   |  |
| CWO1 and senior                         | Six guests and member's vehicle (one). |



|                             |   |
|-----------------------------|---|
| E-6 thru E-9                | Six guests and no vehicle.                      |
| JSDF Academy Staff          | Six guests and member's vehicle (one).          |
| E-5 and E-4                 | Four guests and no vehicle.                     |
| E-3 and junior              | Two guests and no vehicle.                      |
| JSDF Academy Student        | Six guests and no vehicle.                      |
| <b>Complimentary Guests</b> |   |
| Command Guest Pass Holders  | Six guests and his/her/company's vehicle (one). |

7. Satellite Area Access

a. DBIDS capabilities are limited to Main Base. Therefore, FLEACT Yokosuka satellite areas may only issue Escort Only passes. All unescorted requirements must be processed through the VCC at Main Base. Legacy passes issued at satellite areas will only be accepted at the satellite area that issued the pass. DBIDS cards and passes will be accepted at satellite areas.

b. Ikego Housing Area. Ikego residents may request and receive escorted one-day and 72-hour over-night passes for their guests from the Ikego Security Office. Due to the location of the Security Office, the following procedures will be adhered to:

(1) Guest and sponsor will be informed they are required to proceed to Ikego Military Police Headquarters (MPHQ) to apply for, and receive, a pass for the guest.

(2) The guest and the sponsor's information will be logged into the ECP log book and include the contact number and address for the sponsor.

(3) The ECP will contact Ikego MPHQ and inform them of the guest.

(4) MPHQ will receive the guest and let the ECP know they have been received.

(5) Failure to receive a pass will result in an escort violation per this instruction. The guest will be considered a trespasser.

(6) Ikego Housing Area residents with prospective overnight guests staying more than 72 hours are encouraged to apply for an overnight pass with Ikego MPHQ and an overnight unescorted pass through Yokosuka VCC. This will alleviate the need for guests arriving at the airport to report to the VCC immediately upon arrival.

b. Tsurumi and Hakozaki Areas

(1) Escorted or unescorted access is permitted to access these areas and must be processed through the Main Base VCC. These facilities are bulk petroleum storage areas and access is strictly restricted to only those whose official business requires them to be onboard.

(2) In the event a special circumstance arises requiring an escorted access, an official request, (CFAY 5532/24) must be submitted to the VCC from requesting authorities. Once received and verified, the VCC supervisor will contact the JCF supervisors authorizing an escort required pass to be issued for the requested individuals.

c. Urago

(1) Escorted or unescorted access is permitted to access these areas and must be processed through the Main Base VCC. These facilities are Navy Munitions Command ordnance storage areas and access is strictly restricted to only those whose official business requires them to be onboard.

(2) In the event a special circumstance arises requiring an escorted access, an official request, (CFAY 5532/24) must be submitted to the VCC from requesting authorities. Once received and verified, the VCC supervisor will contact the JCF supervisors authorizing an escort required pass to be issued for the requested individuals.

8. Unofficial Visitor Requirements

a. Personal Guest Requirements. U.S. military personnel and their dependents, DoD CAC holders, and specific DBIDS card holders, **who are registered in DBIDS**, are authorized to bring guests on the installation after obtaining a guest pass at the designated location(s). Sponsors are personally responsible for the actions of their guests at all times. Personal guests will not have escort privileges. (Note: Family and/or friends visiting for an official event or function that will be requesting access outside the timeframe of that event will be considered personal guests and must request a DBIDS pass. Example: change of command).

(1) All visitors will be registered in DBIDS. All passes will be issued from DBIDS except for special circumstances that require issue of locally-generated passes. All unescorted passes require a SECNAV 5512/1 and a Personal History Statement (if applicable) at a minimum to be submitted to the VCC with the pass request to initiate a background check.

(2) Paper passes will be issued to those requesting access for 30 days or fewer. DBIDS Cards will be issued to those requiring access for 31 days or more.

(3) Each personal visitor is limited to 60 days total unescorted access in a 365 day period for overnight access, regardless of the sponsor. The 365 day period begins on the first day of the first pass issued. A 30-day extension may be granted with the approval of the FLEACT Yokosuka Security Officer with a valid reason. The Local Nationals who are relatives of the sponsor are eligible to obtain Unofficial Non-Escort Required passes.

(a) All passes with the exception of overnight passes are valid 0500-2359.

(b) Escort Required Passes

1. Will not exceed the expiration date of the landing permission stamp on the passport/residence card of a non-Japanese National or 90 days (including for Japanese residents) whichever is shorter.

2. May be granted overnight access for 72 hours maximum. The sponsor must live in Military Family Housing or be staying with the guest at on-base lodging. After 72 hours, the guest will be required to request unescorted access.

3. Immediate family members who are citizens of designated third countries, as set forth in reference (p), will be escorted at all times.

b. No Escort Required Passes (Unescorted)

(1) Establishing identity for unescorted access. Identity is established either by presenting one “acceptable credential” or by presenting an acceptable combination of “source identity documents”. Acceptable credentials and source identity documents are listed in Section 23.

(2) Acceptable credentials and source identity documents must:

(a) Be original and current (unexpired).

(b) Not contain the markings “Not Valid for Federal Purposes,” “Not For Use as Federal Identification,” “Federal Limits May Apply,” or any other similar phrase.

(c) In the case of a driver’s license or non-driver’s identification card issued by a U.S. state, territory, possession, or the District of Columbia, be compliant with the REAL ID Act of 2005.

(d) Individuals holding more than one acceptable credential must use the credential most accurately depicting the capacity in which the individual is acting for the specific visit to the installation.

(e) The sponsor of the Unofficial No Escort Required pass must be presently stationed at FLEACT Yokosuka or currently under TAD/TDY orders to FLEACT Yokosuka.

Note: When a SOFA member is a patient in NAVHOSP Yokosuka, and sponsor's station is not at FLEACT Yokosuka, upon approval of NAVHOSP Yokosuka, they are allowed to request an Unofficial Unescorted pass during the hospitalization.

(f) Not exceed the expiration date of the landing permission stamp on the passport/ Japanese Residence card.

(g) Unofficial No Escort Required passes may be granted for overnight access for a maximum of 60 days. Extensions may be granted for up to 90 days. For No Escort Required

passes with overnight privileges, the sponsor must live in Military Family Housing, or be staying at the Storks Nest or in on-base lodging. VCC Clerks will verify where the member lives.

(h) Unofficial No Escort Required passes without overnight access may be granted for visitors in a tourist status. The visitor must be able to provide a valid tourist visa. The pass will not exceed 60 days. Extensions may be granted for up to 90 days. Access times will be from 0500-2359 daily.

(i) All visitors arriving after VCC closure will obtain passes at the Carney Gate Guard Supervisor's office. The sponsor must be present with the visitor, providing all documentation required to access the installation.

(3) Action. To request a pass, sponsors must present an Installation Access Request, SECNAV 5512/1 and a Personal History Statement (as applicable) to FLEACT Yokosuka VCC at least five business days (30 days for guests in reference (b)) prior to the guests' anticipated arrival.

(a) For those staying in on-base lodging, a reservation or registration card must be submitted with the Installation Access Request.

(b) Guests must accompany the sponsor when picking up the pass. The guest will provide proper identification, proof of visa status or residency status (if applicable) and complete the DBIDS registration process.

(c) Extension requests must be received 10 days prior to the expiration of the current pass. The FLEACT Yokosuka Security Officer is the approving authority for extension requests. However, requests extending beyond 90 days must be approved by the Installation Commander.

(4) Pre-Authorized Pass. Pre-Authorized Passes are for official visitors, unofficial visitors, personnel whose guest(s) depart and return on a Morale, Welfare, and Recreation tour between 2300 and 0700, guest(s) arriving on the airport shuttle bus at Womble Gate, or personnel desiring to escort more than the allowed number of guests based on paygrade (up to 10 guests per sponsor for special events). Passes will be issued to the sponsor by a gate guard. Submit a "Pre-Authorization Pass Request Form (CFAY 5532/24)" along with a copy of guest's ID to the VCC at least 72 hours prior to the guest's anticipated arrival. The sponsor can pick up the approved pre-authorized pass from the VCC prior to arrival or the ECP whichever mentioned upon arrival. After proper identification, the guest, escorted by the sponsor, will be allowed to access the installation. The sponsor will constantly escort their guests while on-base.

## 9. Official Visitor Requirements

### a. Official Guests Escorts

(1) Personnel with a valid DoD CAC, JMDSF personnel, and specific DBIDS card holders, **who are registered in DBIDS**, are authorized to escort up to eight official guests and three vehicles. Other approved official escorts are specified in this section.

(2) Foreign military members, foreign civilians and, in certain accompanied circumstances, their families, are required to be vetted through the Multiple Threat Alert Center (MTAC).

(a) The sponsoring organization is responsible for notifying the FLEACT Yokosuka Security Officer of all approved requests of foreign military members, foreign civilians, and their families.

(b) The sponsoring organization is responsible for notifying U.S. Naval Forces Japan N5 of all official foreign visitors who are not Japanese nationals requesting access to the installation no later than 21 days prior to their arrival. Records must be maintained of foreign visits which have not been processed through the MTAC. It is the sponsoring organization's responsibility to ensure the visit is properly recorded and documented when official foreign visitors arrive and depart the installation.

b. Newly hired personnel (MLC/IHA employees) are processed through the Human Resources Office (HRO). HRO provides all base access requirements to the VCC for processing. Once personnel have met all screening requirements, the newly hired personnel may request an unescorted two week pass while awaiting their official credentials (e.g. CAC).

c. Official Visitor Passes. All visitors will be registered into DBIDS. All passes will be issued from DBIDS except for special circumstances which require the issuance of locally-generated passes. All unescorted passes require a SECNAV 5512/1 form and a Personal History Statement (if applicable) at a minimum to be submitted to the VCC with the pass request to initiate a background check.

(1) Paper passes will be issued to those requesting access for 30 days or less. DBIDS cards will be issued to those requiring access for 31 days or more. Personnel needing 30 days or fewer, but who perform work in the elements may request a DBIDS card.

(2) All passes with the exception of overnight passes are valid 0500-2359.

(3) Escort Required Passes

(a) Does not give vehicle or personnel escort privileges, but may have vehicle access privileges.

(b) Will not exceed the expiration date of the landing permission stamp on the passport or Japanese Residence card.

(c) Will only be issued for the timeframe of official duties as requested by the sponsoring command or company.

(d) Per reference (r), Local Hired Contractors who visit daily can receive a multi-day pass even though the escort may change. The escort must be an employee from the sponsoring command/company.

(4) No Escort Required Passes

(a) Will not exceed the expiration date of the landing permission stamp on the passport or Japanese Residence card.

(b) Will only be issued for the timeframe Monday through Friday of official duties or 0500-2359.

(5) DBIDS Card. DBIDS ID Cards will be issued to personnel who require access for 31 days or more. **Cards will not exceed two years**, or the length of the contract or immigration visa, whichever is shorter.

(a) Official DBIDS cardholders can be escorted or unescorted and the hours allowed for access will be provided from the requesting command. Standard access is 0500-2359 in Force Protection Conditions Normal through Bravo. Holders of Official No Escort Required DBIDS Cards who can be granted escort privileges are limited to local contractors who are registered based on the procedure stated on the reference (s) and who have also completed their background checks. Other official DBIDS Cards include, but are not limited to, the following categories:

1. Medical. DBIDS cards are issued to local and foreign national medical observers at NAVHOSP Yokosuka, upon written request from the Chief of Medicine, for a specified time.

2. Religious. DBIDS cards are issued to personnel sponsored by the Command Chaplain.

3. Education. Persons having an affiliation with the DoD Education Activity or Navy College either as tuition paying parents, students, administrators, instructors and substitute teachers, aids or as educational volunteers for a specified period of time not to exceed one year may apply. This category does not include guest speakers.

4. Technical Representatives. Persons serving as technical advisors and representatives of private U.S. or Japanese companies for a specified period of time not to exceed one year may apply. This category is extended to U.S. contractors who represent companies having a company name that does not appear in the authorized contractor register. It also extends to persons who are not personally registered in the Contractor Vetting System.

5. Other Volunteers. Persons who serve as volunteers and who are invited by Commander, FLEACT Yokosuka or from among one of its tenant commands for special purposes, such as, but not limited to, personnel exchange programs and Camp Adventure programs, for a specified period of time not to exceed one year may apply.

6. Other Long-Term Visitors. Persons who are not listed in the previous categories as requested by FLEACT Yokosuka or one of its tenant activities for special purposes for a specified period of time not to exceed one year may apply.

(b) Temporary access

1. Newly hired personnel who are U.S. citizens and their command sponsored family members awaiting CAC/ID cards will be issued a two-week unescorted pass under the following conditions:

- a. The employee is on official orders.
- b. The employee provides a valid Navy Lodge or Navy Gateway Inns and Suites registration card with the number of guests required to receive a pass.
- c. The sponsoring command/organization escorts the personnel requiring a pass to the VCC.

2. Newly hired personnel, excluding U.S. citizens and those listed in reference (p) being processed for base access through HRO may receive temporary access per reference (q) as long as they meet the following conditions:

- a. Submission of required base access documents.
- b. Satisfactory completion of name checks against the debarment list, Consolidated Law Enforcement Operation Center, National Crime Information Center, and any other locally available records.
- c. Processing of security checks for persons granted temporary access will be expedited.

(c) Per reference (q), contractors with SOFA status performing work on the installation must present a renewed and valid Letter of Authorization (LOA) in order to obtain a DBIDS pass. The LOA does not replace any existing required documentation for access control.

(6) Pre-Authorized Pass. Pre-Authorized Passes may be used for commands or personnel desiring base access for individuals or groups making official or courtesy calls. Requests will be made using a Pre-Authorized Pass Request (CFAY 5532/24) or memorandum stating the names, date of birth and nationality of the individuals visiting, purpose of the visit, time and date of arrival and anticipated departure, vehicle description, license plate number, name, grade, and

telephone number of the escort. Sponsors for unofficial purposes may escort up to 10 guests at a time. Commands sponsoring guests for official purposes will limit the number of guests to that which the escorts can reasonably regulate. All guests must be escorted while on-base. The sponsor can pick up the approved pre-authorized pass from the VCC prior to arrival, or at the ECP upon arrival. After proper identification, the guest with the sponsor will be allowed to access the installation. The sponsor will constantly escort their guests while on-base. Pre-Authorized passes are limited to only one day; overnight staying on base is prohibited.

(7) Entry of Tourists and Tour Groups. Tourists and tour groups may contact the FLEACT Yokosuka Public Affairs Office to arrange tours. Under normal circumstances, 14 working days are required.

#### 10. Contingency Plan for Non-DBIDS Use

a. With the exception of satellite areas, the following will be implemented during periods when DBIDS is not operational:

(1) Guests that have provided all required documentation to include the access request will be provided a locally generated pass. All guests requesting unescorted access must provide a completed SECNAV 5512/1 to receive a background check, even when utilizing legacy passes.

(a) If the request was for overnight access, a legacy pass will be issued for 24 hours and the guest and sponsor must return to the VCC the following day to complete the registration process in DBIDS. Under extenuating circumstances, passes may be extended only after approval from the FLEACT Yokosuka Security Officer.

(b) If the request was not for overnight access, a legacy pass will be issued for 7 days or until the system is restored. The guest must return to the VCC to complete the registration process in DBIDS.

(2) Guests who have not provided all required documentation prior to the DBIDS outage will fill out a Pre-Authorized request and receive either a legacy pass for 24 hours for overnight access or a pass that expires at 2359 daily for 7 days for access without overnight privileges. Upon system restoration, guests will be required to return with their sponsors and provide the Installation Access Request form and complete the DBIDS registration to receive a DBIDS pass for the remainder of their requested time.

b. When the VCC closes, the Guard Supervisor at the Carney Gate ECP will issue legacy passes. No one-day passes will be issued after 2200. Therefore, this is only for extenuating circumstances, such as guests staying overnight on the installation arriving late due to a delayed flight.

c. Womble Gate Pass Office



(1) All commercial vehicles must enter through Womble Gate from 0600 to 1800 with the exception of off-base taxis. Requests to enter FLEACT Yokosuka after hours must be submitted to the VCC at least three business days prior to the visit.

(2) Contractor one-day passes may be issued at Womble Gate only for those driving commercial vehicles and during times directed by the FLEACT Yokosuka SO. At no time will any visitor use the Womble Gate Pass Office to avoid registering in DBIDS.

#### 11. Multi-Installation Access

a. Possession of a valid/authorized credential does not automatically authorize access to multiple installations. DBIDS provides the ability to grant access to multiple installations to individuals with a valid/authorized credential without issuing separate credentials for each installation. Multiple DBIDS cards or a combination of DBIDS card and CAC will not be issued for one individual to access multiple installations.

b. GOJ, JSDF, UNC(R), third country military personnel with written support from UNC(R) and U.S. Embassy personnel may enter the installation using their organization's official credentials. However, in order to escort visitors on the installation, they must have either a DBIDS card or CAC.

c. DBIDS cards issued by another installation will only be accepted after initial registration with the VCC. The VCC will provide Government Official access, but cannot change the escort permissions on a card issued by another command. The VCC and the ECPs are responsible for ensuring compliance with FLEACT Yokosuka policy within the limitations of the DBIDS system (example: Yokota Air Base issues credential to an individual and limits the personnel escort privilege to four. FLEACT Yokosuka allows for up to eight personnel, but the DBIDS system will only allow for four sponsored visitors. Therefore, the individual is limited to four while at Yokosuka). If a DBIDS card issued from another installation prevents personnel from carrying out orders, a DBIDS paper pass can be issued in 30-day increments (example: the issuing installation set escort and vehicle privileges to zero, but orders state a rental car is necessary).

d. When granting access to FLEACT Yokosuka, the duration will be limited to the length of the orders or up to one year maximum regardless of the credential issuer's policy and duration of the credential.

e. MLC/IHA employees, with the exception of personnel whose nationality is designated in reference (p), assigned under USFJ but not to FLEACT Yokosuka who are on temporary assignment to a specific command may be granted access using a CAC or DBIDS card issued by their parent installation. They are authorized to enter and exit the base via the Carney, Womble, and Verney Gates.

#### f. Access Procedures

(1) CAC Access

(a) Visitors are required to present their CACs to the VCC with a copy of their TAD/TDY/Information Technology (IT)/Training orders. Access will only be granted for the specific period indicated on the TAD/TDY/IT/Training orders.

(b) If they are not under TAD/TDY/IT/Training orders, they must be sponsored and provide an Installation Access Request or an official letter from the sponsoring command with the access timeframe required.

(c) CAC holders accessing the base by a government vehicle for official duties must have their sponsoring command located onboard FLEACT Yokosuka contact the VCC with dates of access required and names of individuals accessing the installation. The visitors must be registered in DBIDS and can be granted access prior to arrival. If the visitors are not registered in DBIDS, they will be required to stop at the VCC immediately after entering the installation.

(2) DBIDS card Access. FLEACT Yokosuka procedures require DBIDS cards and passes to contain remarks to identify the holder as having unescorted or escort required access. Unescorted access must be identity proofed, vetted and receive fitness determination per Navy policy. Not all USFJ installations have the same requirements.

(a) DBIDS card holders must be able to provide documented proof of a favorable background investigation to receive unescorted access to FLEACT Yokosuka in addition to TAD/TDY/IT/Training orders, an Installation Access Request or an official letter requesting access.

(b) If an individual can provide documentation or proof of a favorable background check, access will be granted on the current DBIDS card that was issued by their parent installation.

(c) If an individual cannot provide documentation of a favorable background check, the individual will be issued a DBIDS pass for the period of access required. The installation access request and the SECNAV 5512/1 must be completed and submitted by the sponsoring command to the VCC for unescorted access. Escorted access will only require the installation access request.

12. Designated Third Country Nationals (DTCN)

a. Restrictions on DTCN. Individuals whose nationality is designated in reference (p) are restricted from accessing FLEACT Yokosuka unless approved by the Installation Commander.

b. Sponsors requesting access for guests must complete SECNAV 5512/1, a Personal History Statement and Installation Access Request with a copy of their passport 30 business days prior to the guest's anticipated arrival.

c. NCIS FEFO conducts background checks via the MTAC on all DTCN requests.

d. Non-family member DTCN guests, if approved, will constantly be escorted and are not authorized on base between the hours of 2359 and 0500.

e. Immediate family members of the sponsor or sponsor's spouse (parents, grandparents, siblings and siblings' minor children) who are DTCNs, if approved, may access the base and have overnight access as long as they are constantly escorted by their sponsor. VCC may request additional documents to verify their relationship to the sponsor. The burden of proof for such relationships falls on the sponsor.

f. DTCN school children and school officials who are attending a Department of Defense Education Activity sponsored event are authorized access to the installation as long as they are constantly escorted while on base by SOFA sponsored personnel.

g. Prospective employees. Prospective employees who are DTCNs must submit SECNAV 5512/1, Personal History Statement and Designated Third Country National Prospective Employee request with a copy of their passport to the Visitor Control Center. NCIS FEFO will conduct the background checks and forward a recommendation to FLEACT Yokosuka Security Officer. Employment is not authorized without prior coordination and approval from Commander, FLEACT Yokosuka. Absent unique skills and /or circumstances, the hiring of DTCNs is strongly discouraged. When submitting a request for access for a prospective DTCN employee, the sponsoring activity will submit a statement explaining what necessitates the hiring that person rather than a non-DTCN.

13. Single Source Coordinator. The Single Source Coordinator will be designated in writing by the Installation Commander to perform the following duties:

a. Oversees the registration and clearance of vendors, contractors, and drivers providing transportation services, e.g., taxicab, limousine, ride share, and shuttle services.

(1) Military Liaison And Civil Affairs Director is the designated approving authority for business entities operating transportation services on the installation.

(2) Verifies transportation service vehicle operators have completed appropriate vetting and met fitness standards for installation access.

(3) Collects expired passes within one working day of notification, and conducts quarterly reviews with transportation service companies to verify drivers' continued employment with the company.

(4) Coordinates issues between the installation Security Department and contractors.

b. Contracted Transportation Services. The Installation Commander may restrict access at heightened FPCON and must ensure that registered companies understand that their access may be restricted due to a change in security conditions.

(1) All taxi/transportation companies are permitted to apply for installation access.

(2) The SSC will facilitate the registration requests of transportation service companies to conduct business on an installation.

(3) All transportation service vehicles will be licensed to operate and provide transportation services by the as required by Japanese law.

(4) All transportation service vehicle operators will be:

(a) Properly licensed to operate a vehicle for hire and possess a current Japanese or SOFA driver's license.

(b) Identity proofed, vetted, and fitness determined prior to allowing access to the installation.

(5) All transportation services operated on the installation will be by an authorized driver possessing a CFAY-issued DBIDS credential.

(6) The Installation Commander will restrict transportation service contractor/companies from areas that include high-value assets and restricted areas. Service providers should be limited to movement to and from fare pickup and drop-off destination.

(7) The Installation Commander will inform registered transportation service companies that any violation of federal law, base regulation, or other disruptive activity will result in the termination of that company's access under this program.

(8) The Installation Commander may establish programs for unregistered transportation service companies, or rideshare programs (e.g., Uber, Lyft). If the SSC has not registered a transportation service or rideshare, the following conditions apply:

(9) The transportation service vehicle operator will meet all requirements in Section 16.

#### 14. DBIDS Categories

a. DoD categories correspond to a CAC holder's Defense Enrollment Eligibility Reporting System affiliation. DBIDS contains the same categories to use when issuing DBIDS cards. Categories are fixed and cannot be modified. DBIDS categories will be assigned to DBIDS cards as close as possible to CAC assignments. Each category is color-coded the same as CACs as seen in the table below.

b. Sponsoring commands are responsible for officially reporting the names of emergency essential personnel to ensure they receive the correct category and access permission.

| DBIDS 5 CATEGORY         | SPONSOR  | CFAY VISITOR   |
|--------------------------|----------|--|
| Conveyance               | COMMAND  | Transportation Services/Taxi Drivers (U.S. Citizen)                                  |
| Emerg Essential Civilian | COMMAND  | U.S. and Non U.S. Civilians and Contractors Identified as Emergency Essential or     |
| Facilities Service       | N/A      | To be identified for later use.  |
| Facility Use             | COMMAND  | Gold Star Family Members   |
| Foreign Civ Visitor      |          | Non-U.S. Citizen Visitor   |
| Foreign Gov Civ          | COMMAND  | Non-U.S. Citizen Government Official   |
| Foreign Gov Contr        | COMMAND  | Local National Employees/Local Contractors (including other categories, ie. Non-U.S. |
| Foreign Mil Dependent    | PERSONAL | JSDF and other Foreign Military Members like   |
| Foreign Mil Retiree      | PERSONAL | UN ID holders  |
| Foreign Military         | PERSONAL | U.S. Citizen Visitor 31 days or more.  |
| Long Term Visitor        | PERSONAL | To be identified for later use.  |
| Maintenance              | N/A      | To be identified for later use.  |
| Other                    |          | Special Circumstance (Children) – U.S.   |
| Personal Delivery        | N/A      | To be identified for later use.  |
| Personal Services        | N/A      | To be identified for later use.  |
| Privatized Housing       | N/A      | To be identified for later use.  |
| US Gov Civilian          | COMMAND  | U.S. Gov Civilian  |
| US Gov Contractor        | COMMAND  | U.S. Gov Contractor 31 days or more.   |

#### 15. Denial of Access

a. Permanently Disqualifying Fitness Determination Standards that may not be waived by the Commander, FLEACT Yokosuka or designated representative. Disqualifying conditions include being identified or registered in the Foreign Fugitive File, Immigration Violator File, Naval Sex Offender Registry Database or Known or Appropriately Suspected Terrorist File, and felony convictions for rape, child molestation, trafficking in humans, espionage, sabotage, treason or terrorism. The VCC will deny these requests.

b. Disqualifying Fitness Determination Standards that may be waived by the Commander or a designated representative. The VCC will brief these findings to the Security Officer, SJA, Chief Staff Officer and the Installation Commander for approval or disapproval of base access.

(1) Other Felony Convictions. Other than the disqualifiers listed above, any felony conviction within the past 10 years is grounds for denying installation access. The Installation Commander may waive this requirement. Felony convictions more than 10 years old, except for those identified above, do not require a waiver.

(2) Wanted Persons (active wants/warrants), persons on the Debarment List, persons released from prison or on probation within 5 years after a felony conviction or persons identified in the Violent Person Crime File will not be granted access to the installation.

(3) Arrests for a disqualifying event without disposition (conviction, dismissal, not guilty or acquittal) more than 10 years old are not grounds for denying access.

c. Debarment. The Installation Commander may issue debarment letters to deny an individual access for involvement in the commission of a criminal offense, when access is inconsistent with the interests of national security, when personal conduct reflects negatively on the image of the U.S., or when access adversely affects the health, safety, or morale of personnel on the installation. Debarment letters will be entered into the Consolidated Law Enforcement Operation Center and DBIDS. All guests requesting access will be vetted for debarment. The Debarment List will be prepared by the FLEACT Yokosuka Staff Judge Advocate (SJA). The SJA will give to FLEACT Yokosuka Security Department the Debarment list whenever it is revised, i.e. names are added or removed from the list. FLEACT Yokosuka VCC will update all necessary databases with the Debarment List and ensure base access is restricted from those on the list through CLEOC, DBIDS and any other means available. A paper copy will be with VCC in the event of network outages and VCC will manually check the Debarment List should the need arise. A copy of the Debarment List will be located at the Guard Supervisor Desk and updated by VCC as necessary.

d. VCC clerks may deny access for falsification or failure to provide required information on required documentation to include falsification or forging signatures. Handwritten and electronic signatures are both acceptable on SECNAV 5512/1.

e. Individuals who cannot provide proper identification will be denied access, unless otherwise stated in this instruction.

f. Those who refuse to register their personal information with DBIDS will be denied entry.

g. Individuals with previous escort violations may be denied access.

h. The Installation Commander may deny access for other reasons based upon the recommendation of the Security Officer and the SJA.

i. Those personnel who have been denied access but wish to appeal must coordinate with the FLEACT Yokosuka SJA for base access prior to attempting to access the installation.

## 16. Temporary Vehicle Access

### a. Temporary Vehicle Access

(1) All vehicles will be registered into the DBIDS.

(2) The VCC may issue no more than a three day vehicle pass for Privately Owned Vehicles (POV) to authorized personnel. Any vehicle pass greater than three days must be issued at the FLEACT Yokosuka Vehicle Registration Office (VRO). All vehicles must have current registration requirements per reference (f).

(a) When VRO is closed, U.S. military personnel who are in the process of registering their POVs will be issued a vehicle pass dated until the next VRO working day.

(b) If the registered owner of the vehicle is not U.S. military personnel, the number of vehicle passes issued will not exceed five per month. The driver must have written permission from the owner to operate the vehicle.

(c) If the sponsor is away from Yokosuka, e.g. underway or on TAD, and the spouse is requesting a vehicle pass, the spouse must present a copy of the sponsor's current orders.

(d) Personnel driving a commercial rental vehicle and who are staying on the installation will obtain a vehicle pass issued for the duration of the visit by VRO. When VRO is closed, a vehicle pass will be issued dated until the next VRO working day. If the driver is transferring, they must present supporting documents of permanent change of station orders and a valid Navy Lodge or Navy Gateway Inns and Suites Registration Card.

(e) Personnel under TAD/TDY orders are authorized to obtain a One-day Vehicle Pass if TAD/TDY orders indicate authorization to drive a vehicle. Personnel must have a valid international driver's license or SOFA license. A temporary vehicle pass will be issued at VRO.

(f) All guests requesting vehicle passes must be relatives of the sponsor or sponsor's spouse and meet the above requirements.

(g) A one-day pass will be issued to all authorized dealers not to exceed a total of two vehicles for sale on the installation at a time. Authorized dealers must have FLEACT Yokosuka Morale, Welfare and Recreation (MWR) passes to park vehicles for sale in the MWR sale lot.

(3) Vehicle passes for local contractors and official guests. The requesting command will be responsible for the following:

(a) All commercial vehicles must enter through Womble Gate from 0600 to 1800 with the exception of off-base taxis. Requests to enter FLEACT Yokosuka after hours must be submitted to VCC at least three business days prior to the visit. Oversized vehicles are required to enter the installation at 0400 through the Carney Gate outbound lane. The sponsoring

command for oversized vehicles must coordinate with FLEACT Yokosuka Security Department to ensure safe and proper access.

(b) All vehicles entering and exiting the installation are subject to search at all times by FLEACT Yokosuka NSF. All drivers must obey NSF verbal directions during vehicle inspections.

(4) Authorized off-base taxi drivers will be issued DBIDS cards for a period of one year. Taxis are authorized to wait for customers at either the Carney Gate or Commissary Taxi Stands. Taxi drivers may not solicit customers at any other locations. The taxi company is required to immediately inform the VCC and VRO of any changes of their drivers' statuses. Taxis are authorized to enter FLEACT Yokosuka as set forth below:

(a) During the hours of 0500-1800 all taxis will enter through the far left inspection lane at Womble Gate and be inspected by the ECP sentry.

(b) During the hours of 1800-0500 all taxis will enter through Carney Gate and be inspected by the ECP sentry.

(5) Local hired employees are not authorized to obtain a Vehicle Pass issued from VCC for commuting purposes.

(6) Companies that are authorized to conduct business on FLEACT Yokosuka, are required to register their vehicles at FLEACT Yokosuka VCC. Only vehicles registered to companies may be driven by the authorized drivers of that particular vehicle while onboard FLEACT Yokosuka. VCC will only issue long term vehicle passes to local contractors. Any long term pass for a privately owned vehicle will be obtained from VRO. Overnight parking on-base is not permitted unless pre-authorized by FLEACT Yokosuka.

b. Registration requirements. A FLEACT Yokosuka Vehicle Pass (CFAY 5800/16D) will be issued (if approved) upon presentation of the following documents to the VCC Office:

- (1) FLEACT Yokosuka Contractor Gate Pass.
- (2) Valid Japanese driver's license.
- (3) Vehicle Registration (Proof of ownership of the vehicle owned by company, or contractor if needed).
- (4) Proof of insurance (JCI).
- (5) Request for registration of commercial vehicle (CFAY 5800/49).



Note: Vehicle passes will not exceed 1 year regardless of the length of the contract. If the vehicle registration/Insurance/Documentation expires before then, the pass can only be issued to the date of expiration.

c. Weight Handling Equipment. All cranes and associated rigging gear, must conform to applicable Japanese regulations and NAVFAC P307 (Management of Weight Handling Equipment Manual) and display a certificate of compliance in their cab prior to entry on FLEACT Yokosuka. Please see the CFAYINST 11262.1B for further guidance.

d. Reporting Changes. Base contractors that have any changes in their company, contract or vehicle status are required to report these changes to FLEACT Yokosuka VCC. Final authority belongs to the Installation Commander regarding issuance and termination of FLEACT Yokosuka vehicle passes.

e. Re-issuance of lost vehicle pass. If a vehicle pass is lost, stolen or damaged before expiration, the pass holder will need to submit 5532-54 (Rev 12-19) Lost Report Form to VCC for re-issuance.

## 17. Violation Policy

a. Unescorted Guests. If “Escort Required” guests are found unescorted, for the first violation, the sponsor’s escorting privileges for all passes will be suspended for 30 days. A second violation will result in a one year suspension. Installation access for the guest will be suspended until further notice. If the sponsor desires to appeal the suspension, the sponsor must send a written request to the FLEACT Yokosuka Legal Office explaining their circumstances.

b. Unescorted DTCN Guests. If DTCN guests are found unescorted, the sponsor’s escorting privileges will be revoked immediately and installation access for the guest will be suspended until further notice.

c. Over Stay. If guests are found on the installation beyond the time allocated for their pass, the sponsor’s escorting privileges for all passes will be suspended for 30-days for the first violation. A second violation will result in a one year suspension. Installation access for the guest will be suspended until further notice.

d. Trespasser. If personnel enter the installation without proper authorization, the violator will be escorted off the installation by NSF members. If a sponsor is involved, their escorting privileges will be revoked immediately and installation access for the guest will be suspended until further notice.

e. Mutilated or Tampered Passes. Any passes issued by U.S. FLEACT Yokosuka are prohibited from being mutilated or tampered with. The sponsor’s escorting privileges will be revoked immediately and installation access for the guest will be suspended until further notice.

f. Personnel who attempt or admit to attempting to maliciously circumvent the escort privileges, to include the maximum number of guests allotted, will have their escort privileges suspended for 30 days. All current passes under the sponsor will be terminated. Additionally, sponsoring commands will be notified of further administrative or legal actions.

g. Any violations of the guest policy will affect the violator, sponsor, and sponsor's dependents. A record of the violation will be kept on file for three years at VCC.

h. Traffic Violations. Per reference (t), traffic violations resulting in a traffic citation issued by FLEACT Yokosuka Security Department are a basis for loss of driving and/or guest privileges. For guests, the first violation will result in suspension of driving privileges for 30 days and the second violation will result in suspension of base and driving privileges until further notice. Patrols must ensure the VCC is contacted when guests with a one-day vehicle pass receive a traffic violation. VCC personnel will annotate the suspensions under the guest's profile in DBIDS.

#### 18. Procedure In Case Of Loss of Credentials

a. Persons who cannot account for the location of their CAC/DBIDS card must immediately notify FLEACT Yokosuka NSF to report the CAC/DBIDS card as either lost or stolen.

b. MLC/IHA/HPT/PSC CAC/DBIDS card holders who report their CAC/DBIDS card as being left, lost or stolen will be governed by the following:

(1) CACs that are lost or stolen. The employee may be issued a temporary DBIDS unescorted visitor pass at the VCC after verification of his/her working status by VCC personnel. The employee must report to the Japanese police or FLEACT Yokosuka Security Department immediately and he/she will submit a Lost Report (CFAY 5532/54) to FLEACT Yokosuka Security Department. The employee must request PSD to reissue the CAC.

(2) DBIDS cards that are lost or stolen. The employee may be issued a temporary DBIDS unescorted visitor pass at the VCC after verification of his/her working status by VCC personnel. The employee must report to the Japanese police or FLEACT Yokosuka Security Department immediately and he/she will submit a Lost Report (CFAY 5532/54) to FLEACT Yokosuka Security Department. The employing activity will request to reissue a gate pass for the employee utilizing a Request to Reissue Gate Pass for Employee Form (CFAY 5532/56) and forward the form to VCC. Upon receipt of the request, VCC staff will arrange reissuance of the DBIDS card immediately.

(3) CAC/DBIDS cards that are left at home or place of work. The employee may obtain a one-day pass unescorted at VCC after verification of his/her working status by VCC personnel.

c. Contractor/Off-Base Taxi DBIDS card holders who report their DBIDS card as being left, lost, stolen or damaged will be governed by the following:

(1) DBIDS cards that are left at home or place of work. Contractor may enter the base with his/her company escort.

(2) DBIDS cards that are lost, stolen or damaged. The company must report to the Japanese police or FLEACT Yokosuka Security Department immediately and he/she will submit a Lost Report (CFAY 5532/54) to FLEACT Yokosuka Security Department. The company also need to request reissuance of the pass with written documentation. Upon receipt of above two documents, VCC will arrange reissuance of DBIDS cards. Until he/she gets new DBIDS cards, he/she needs to enter the base with his/her company escort. A police reports not required for a damaged pass.

d. Other Official Unescorted DBIDS card holders who lose DBIDS cards. The person who lost the DBIDS card needs to submit a Lost Report (CFAY 5532/54) to FLEACT Yokosuka Security Department. The sponsor needs to re-submit another request for pass reissuance.

#### 19. Authorized Identification For Visitors

a. Identity proofing, vetting and determination of fitness are required in order to approve unescorted access to the installation. Additionally, all guests must be registered and issued a pass from DBIDS, which limits the types of identifications that can be used for registration. While certain identification is approved for identity proofing, in order to complete a background check for vetting and registration into DBIDS, additional forms of identification are mandatory. Required forms of identification are covered in paragraph 4, DBIDS Registration.

b. Identity Proofing. The following credentials are identity proofed at the card issue site from federally authorized identity documents, and will be considered identity proofed. CAC, Uniformed Services ID Card issued to military retirees and military family members, Non-DoD Federal Personal Identification Verification, U.S. Passport or Passport Card, foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa, or others listed in reference (a) and the illustrations below.

c. Vetting and Fitness. The SECNAV 5512/1 is the sole means to initiate background checks on all visitors and/or contractors/vendors. Every background check for the purpose of access control requires completion of SECNAV 5512/1 for accountability purposes. Failure to do so will result in inconclusive results of criminal history and thus denial of unescorted access.

(1) Waiver Process. Personnel who have been initially denied access based on criteria identified in Section 17 may appeal or request a waiver in writing from the Installation Commander. When reviewing criminal history to make a waiver determination, both adverse information and mitigating factors should be considered. The individual requesting a waiver will be notified in writing of the decision within 30 days of package submission.

(a) VCC officials will verbally inform visitors requesting a short-term pass that they do not meet access standards and will explain the process to request a waiver and/or appeal.

(b) FLEACT Yokosuka SO will notify personnel requesting DBIDS credentials in writing within 14 days of their access denial and include the process to request a waiver and/or appeal.

(c) Personnel who have been denied access during periodic re-vetting for the purpose of continued unescorted access may appeal and/or request a waiver from the Commander.

(d) Periodic background screening of personnel. Personnel who have received an approved waiver or appeal will only be re-vetted back to the original date of waiver or appeal plus one year.

(e) The additional year is necessary due to possible reporting delays. If no new disqualifying offense is found, the current waiver can be extended and no new waiver processing is required. If additional disqualifying offenses are found, the entire record will be reviewed.

(f) The Installation Commander or designated representative will determine if access will be granted based on the information submitted for consideration. Until this determination is made, the person's access to the installation will be denied.

(2) Appeals. Any person being denied initial participation in DBIDS or who has their DBIDS privileges suspended or revoked for any reason, may appeal the denial/suspension/revocation.

(a) Vendor or contractor employees may initiate the adjudication process when a background screen failure results in disqualification from participation in DBIDS and the vendor or contractor employees do not agree with the reason for disqualification. The adjudication process must be initiated within 30 days of receiving written notice of disqualification. Vendor or contractor employees may apply for a waiver when a background screening failure results in disqualification from participation in DBIDS. The waiver process must be initiated within 60 days of receiving written notice of disqualification. People on the Sexual Offenders Register will not receive a waiver.

(b) All waiver requests will be initiated with the Security Officer. The Installation Commander will be the final waiver determination authority.

(c) The Installation Commander will consult with the installation SJA when determining suitability.

(3) Periodic Screening Requirements. Once an access credential is issued, fitness is not normally determined again until the credential expires and a new credential is issued.

#### d. DBIDS Registration

(1) U.S. Citizen. In order to register a visitor into DBIDS, the visitor must have an ID with an associated ID number. U.S. Citizens are required to provide their SSN, Certificate of

Naturalization or Taxpayer ID Number to receive a DBIDS pass to access the installation. Additionally, passports are required in order to verify immigration visas.

(2) Japanese Residents. In order to register Japanese residents into DBIDS a passport number, driver's license or a My-Number card is required. If the applicant does not have a physical card, the "My-number notification" card will be accepted with another form of acceptable identification shown below. Authorized secondary identifications to access base shown below maybe use for identification in combination with their DBIDS pass to enter the installation.

(3) Non-U.S. Citizen and Non-Japanese Residents are required to provide a current passport with a valid immigration or landing visa for both identity proofing and registration into DBIDS.

(4) Special IDs. Personnel who possess a special Japanese resident card who are not Japanese Nationals must provide a passport. The name on the special resident card must match the name on the passport.

e. Source Identity Documents. All source identity documents must be visually inspected for known security features, as applicable, and for signs of alteration or counterfeiting. Electronic verification is not required for source identity documents, but may be performed if it is available. Unless otherwise specified in this section, source identity documents establish only identity.

20. Authorized Identification Cards of Use at Visitor Control Center: See following figures.

a. Figure 1: Samples of proper identification for DBIDS guest passes. An individual must present one of the below listed official IDs.

|   |  |
|---|--|
| <p><b>My Number Card<br/>(Kojin Bango Card)</b></p> <p><b>Pictured Form Only</b></p>   | <p><b>Japan/Foreign<br/>Passport</b></p> <p><b>Valid Landing permission stamp<br/>required for non-Japanese</b></p>  <p>(Unexpired<br/>visa)</p>           |
| <p><b>Japanese Driver's License</b></p> <p><b>Must have additional<br/>Documents<br/>See next page</b></p>   | <p><b>Resident Card<br/>(Special Permanent Resident card is<br/>also acceptable)</b></p> <p><b>Both visa and expiration date must be<br/>valid.</b></p>  |
| <ul style="list-style-type: none"> <li>❌ ID is not required for minors under 12 years old.</li> <li>❌ Non- Japanese nationals must present passport or resident card.</li> <li>❌ US citizens must provide full SSN.</li> <li>❌ Note: Minor 17 years and younger must be escorted by their parent, or approved guardian after 1700. Approved guardian must provide Guardian Agreement Form</li> <li>❌ For a Japanese driver's license, see next page.</li> </ul> |  |

b. Figure 2: Supplements that are needed to be provided with a Japanese Driver's License in order to get a DBIDS guest pass.

## Supplements for Japanese Driver's License



One of five documents below

#1

**Basic Resident Registration Card (Jumin Kihon Daicho Card)**  
Pictured Form Only



#2

**Address Certificate (Jumin-hyo) With Permanent address (Honseki)**  
Obtain After Identification Issuance  
Valid until expiration of Identifications  
住民票 (本籍入り)



#3

**Family Certificate (Koseki) For whole family / Individual (Koseki Zenbu-jiko Shomei/Kojin Jiko Shomei)**  
Obtain After Identification Issuance  
Valid until expiration of Identifications  
戸籍全部事項証明/個人事項証明



#4

**Kisai Inji-Hyo Record on Drive's license**  
The title must be:  
記載印字票








#5

**Honseki Kakunin Yoshi Record on Drive's license**  
The title must be:  
本籍確認用紙



c. Figure 3: Additional acceptable identification for pre-authorized passes, family escort day, special events or other pre-determined situations.

|   |   |  |  |
|---|---|--|--|
| <p><b>Basic Resident Registration Card (Jumin Kihon Daicho Card)</b><br/><b>Pictured Form Only</b></p>   | <p><b>Student Identification of College or University</b><br/><b>Must have additional documents</b></p>  | <p><b>#1</b></p> <p><b>Address Certificate (Jumin-hyo) With Permanent address (Honseki)</b><br/><b>Obtain After Identification Issuance</b><br/><b>Valid until expiration of Identifications</b></p> | <p><b>#2</b></p> <p><b>Family Certificate (Koseki) For whole family / Individual (Koseki Zenbu-jiko Shomei/Kojin Jiko Shomei)</b><br/><b>Obtain After Identification Issuance</b><br/><b>Valid until expiration of Identifications</b></p> |
| <ul style="list-style-type: none"> <li>•ID is not required for minors under 12 years old.</li> <li>•13~Under 18 years old students may substitute their school IDs. <b>(Pictured only)</b></li> <li>•School ID is acceptable only for Japanese</li> </ul> | <p><b>Physical Disability Certificate</b><br/><b>Must have additional documents</b></p>                | <p><b>+ (plus sign)</b></p>   |    |



d. Figure 4: Acceptable forms of identification to be used for installation access, once given access permissions.

**DBIDS CARD**



**VISITOR PASS**



**DOD CREDENTIALS**



CAC



Uniformed Service ID

**PIV CARD**



**TWIC**



New UniformedService ID

**REAL ID**



**VHIC**



**Front**



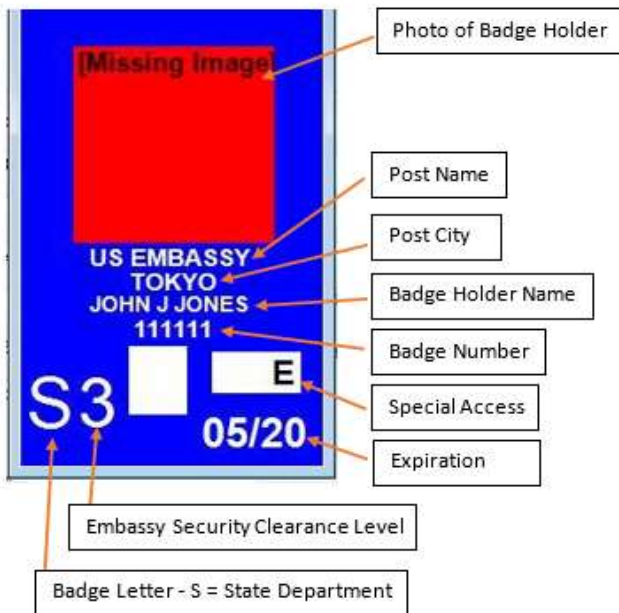
**Back**



e. Figure 5: Contains acceptable forms of U.S. Embassy identification to be used for installation access.

**ACCEPTABLE CREDENTIAL SAMPLES – US EMBASSY**

US Employee Badge   Local Staff Badge



Contractor Badge   EFM Badge



f. Figure 6: Acceptable forms of United Nations Command – Rear (UNC(R)) identification to be used for access to the installation.

ACCEPTABLE UNCR ID CARD SPECIMEN



g. Figure 7: Examples of acceptable credentials that are authorized access with written authorization from UNC(R).



Chapter 12

FORM LISTING

| <b><u>FORM NUMBER</u></b> | <b><u>NAME</u></b>   |
|---------------------------|--|
| N/A                       | Key Inventory Log  |
| N/A                       | Key Control Log  |
| N/A                       | Key Issue Record   |
| N/A                       | Lost Key Report  |
| N/A                       | Key Manufacturing Request  |
| N/A                       | Key Inventory Record   |
| 5532/58                   | Installation Access Request Form   |
| N/A                       | Command Letterhead Request   |
| N/A                       | Request for Joint Use of Local National Employee (MLC/IHA/HPT) Gate Pass to Perform Local Contractor Services                      |
| N/A                       | Base Clearance Request form (Non-local Resident)   |
| 5512/3                    | Request for Temporary Passes With Escort   |
| 5512/4                    | Application for Entry  |
| 5512/19                   | Temporary Pass (Escort Required)   |
| 5512/21                   | Official and Commercial One Day (Gate/Vehicle) Pass Request Form   |
| 5532/1b                   | Official No Escort Required Gate Pass  |
| 5532/24                   | Pre-Authorized Pass Request Form   |
| 5532/25b                  | FLEACT Yokosuka Guest Pass   |
| 5532/25c                  | FLEACT Yokosuka One Day Guest Pass (Official)  |
| 5532/40                   | Japanese Employee Guest Pass Request   |
| 5532/42                   | Nomination of Escort Uncleared Employees   |
| 5532/47                   | Current List of Company Employees  |
| 5532/52                   | Request for Domestic Employee Gate Pass  |
| 5532/53b                  | Base Access Request for Prospective Employee who is a National of Designated Third Country or was born in Designated Third Country |
| 5532/54                   | Lost Report  |
| 5532/56                   | Request to Reissue Gate Pass for Employee  |
| 5700/1                    | Conduct Business within Fleet Activities Yokosuka (Firms Not Located within Japan)   |
| 5700/2                    | Conduct Business within Fleet Activities Yokosuka for Firms Located in Japan   |
| 5700/3                    | Request Gate Pass for Our Employee (New)   |

|          |  |
|----------|--|
| 5800/16b | Vehicle Pass (Womble)                            |
| 5800/16c | Vehicle Pass                                     |
| 5800/16c | Vehicle Pass (VCC)                               |
| 5800/20b | One Day Vehicle Pass                             |
| 5800/20c | One Day Vehicle Pass (Womble)                    |
| 5800/39a | Bicycle Registration Form (MLC/IHA/HPT)          |
| 5800/39b | Request for Registration of Bicycle (Contractor) |
| 5800/46b | Commercial Vehicle Registration                  |
| 5800/48  | One Day Vehicle/Guest Pass Application Form      |
| 5800/49  | Commercial Vehicle Application (VCC)             |

INSERT RESTRICTED CONSOLIDATED RESTRICTED AREA LIST HERE