Marine Transportation Security Clearance Program
Guidance Material – Restricted Area Two Central Controls

New Regulatory Requirement for central controls

329 (4) The following areas shall be established as restricted area two:
(a) areas in the marine facilities set out in Part 1 of Schedule 1 that contain the central controls for security and surveillance equipment and systems and areas that contain the central lighting system controls;

1 Protection of the Restricted Area Two

The Restricted Area Two is a secure area that is intended to ensure the asset is protected from unlawful interference. It is also intended to reduce opportunity for unlawful interference through these key security assets. This could be caused by people, vehicles and/ or equipment, either as the threat itself or as the delivery mechanism for the threat. All of these factors must be considered when identifying a Restricted Area Two perimeter.

2 Application of "Central Lighting System Controls"

- Areas which contain centralized lighting.
- Controls over banks of lighting are included, if they can affect security.
- Individual light switches are not included, unless they can affect security.
- If lighting control has been distributed to more than one centralized area, these smaller centralized areas are included.

    - ***Possible options to address distributed lighting systems include, but are not limited to the following:***
        - designate the surrounding area as a Restricted Area Two; and/or
        - do not designate whole area as a Restricted Area Two, but provide a lockable case or shelter over the controls, and access to that case/shelter would be designated a Restricted Area Two. However security procedures are required to mitigate the risk and persons with the ability to access the area require a security clearance.

- If lighting control is not centralized, this regulation does not apply, however it is recommended that operators use this opportunity to review and determine the threat, as per the security assessment and mitigate as appropriate.

Best practices:
- Any new lighting installations which have centralized controls are located within a security area.
- Back-up systems are in a different location from the main control.

3 Application of "Central Controls For Security And Surveillance Equipment And Systems"

- Controls = the ability to deactivate or modify the parameters / elements of any component of the security system.

- Controls for Security and Surveillance Equipment and Systems for Closed Circuit Television (CCTV), alarms (detection intrusion systems) are included.
- If security and surveillance systems have been distributed to more than one centralized area, these smaller centralized areas are included.
- Central controls for Individual system components are included (eg. CCTV control system), even if they are not in a centralized / common area.
- Individual pieces of equipment are not included (e.g. cameras).

4 Areas of Similar Impact

- Areas that have a similar opportunity to effect security are to be treated in a manner that provides the same level of security. These areas generally offer the same capability. As a result, the impact (and risk) is comparable and failure to apply equal security procedures to both areas means that the less protected one becomes a target (shifting threat).

    - Included as a Restricted Area Two: Back-up sites and Secondary sites.

- Where similar risk exists, but the area is not a Restricted Area Two, facilities will include protective requirements in their security plan for locations other than those identified as being Restricted Area Two. This includes areas which can significantly effect the operations of the facility. This includes systems used for the following purposes:

    - power supplies - These often reside outside of structures but can have the same influence as shutting down the power especially to security and lighting systems;
    - cabling trunks and switches - These are often routed through utility closets, etc. These, if disrupted, can have an impact across a large area;
    - major computer network systems (main and back up) as well as records, such as tape backups;
    - servers with the ability to affect the operation of the facility and those with security data storage;
    - a technological point (e.g. computer, remote dashboards[1]) - where technology exists that would allow the same opportunity to access systems/security data; and
    - communications closets.

    - ***Possible options to address these related security plan issues include, but are not limited to the following:***
        - Monitoring, Locking, Continuous recording, Detection intrusion devices, Tamper resistant seals.

5 Perimeter of the Restricted Area Two

- The perimeter of the Restricted Area Two is the boundary where a demonstrable preventative measure is used to ensure that only persons with security clearances and appropriate authorization are granted access.
- The Restricted Area Two perimeter extends as far as it can be clearly demonstrated that a person does not have the means and the opportunity to affect the central controls.

[1] Dashboard – a system which is separate from the central operation, through which one can have partial or full access to the main system

- The barrier can be determined by asking the following questions:
  - At what location is it determined that a person has a security clearance?
  - At what location is a person without a security clearance stopped from gaining access?
- The barrier (physical limit) must prevent unauthorized entry across the Restricted Area Two operations.
- The perimeter may move with the change in location, size or configuration of the Restricted Area Two.

6 Access control

- The system shall allow only the authorized person(s) to enter.
- Clearance and/or escort and authorization of access need to be granted prior to access to the Restricted Area Two.
- To ensure that the integrity of the security barrier is maintained, there must either be a person present to limit the entry to the validated person or the system must include anti-tailgating and anti-piggybacking measures.
  - Piggybacking is defined as the gaining of entry through security portals by unidentified persons through the conscious assistance of authorized users.
  - Tailgating is defined as the gaining of entry through security portals by unidentified persons without the knowledge of authorized users. This action occurs when an unidentified person follows an authorized user through a portal by following behind and holding the door.

  - ***Possible options include, but are not limited to the following:***
    - Authorized access could include the use of:
      - Access codes, Key control;
      - List of authorized persons / with check at access point (by someone with MTSC); and/or
      - Biometric systems, etc.
    - Anti-tailgating and anti-piggybacking measures options include, but are not limited to the following:
      - Four leaf revolving doors, person-traps and turnstiles.

Best practices:
- Use a combination of options.
- Have an enhanced level of access control for the Restricted Area Two, in comparison to the access control that is in place for the restricted area.
- Use of Biometrics.

7 Consistent level of security:

- Within a secure area, the level of security needs to be consistent, but the manner of obtaining this level may vary according to the marine facility operational requirements.