# STANDARD OPERATING PROCEDURE 119-01-001-02, RESPONSE PROCEDURES FOR SUSPICIOUS PACKAGES, MAIL, OR CORRESPONDENCE

**DEPARTMENT OF HOMELAND SECURITY**

**OFFICE OF THE CHIEF SECURITY OFFICER**

Charles Taylor
Acting Chief Security Officer

3/22/16
Date

# TABLE OF CONTENTS

## 1. PURPOSE

This Standard Operating Procedure (SOP) provides a general structure for the effective operation and administration for the handling of suspicious packages, mail, or correspondence incidents at the Nebraska Avenue Complex (NAC) and off-site locations, to include the residences of senior Department of Homeland Security (DHS) leaders in accordance with 40 U.S. Code § 1315. OCSO's mission is to protect the DHS workforce, property, and information. The Chief Security Officer (CSO) functions as the Designated Official (DO) for the NAC. This SOP explains the basic procedures if suspicious packages, mail, or correspondence are delivered or found and describes who is involved in the response to mitigate the threat and take appropriate investigative action.

## 2. GENERAL POLICY

As part of the CSO's protection responsibility, OCSO has developed the following response capabilities to manage a variety of threats and emergencies. Included in this response, is the need to address threats posed from suspicious packages, to include mail or correspondence directed at DHS senior leaders, employees, and contractors.

OCSO has organized its response to these threats by utilizing two internal units: 1) the Physical Security Division, Force Protection Branch (FPB); and the Internal Security and Investigations Division (ISID). These two units form the primary elements for the initial response to, and mitigation of, potential threats and emergencies posed to staff from suspicious packages.

The United States Secret Service (USSS) continues to coordinate with the DHS OCSO and the DHS Office of the Executive Secretary (ESEC), to address correspondence directed at their Protectees, as defined by their statutory authority under 18 United States (U.S.C.) §§ 3056 and 3056A.

In the event of a threat or incident directed towards a Protectee of the United States Secret Service, the USSS Protective Intelligence Operations Center is immediately notified at 202-406-5000, concurrent with the Secretary's USSS Protective Detail, to activate the appropriate USSS response and/or investigation.

## 3. SCOPE

While this SOP applies to all personnel permanently assigned or detailed to the OCSO, employees and contractors specifically assigned to the OCSO FPB, ISID, and contract Protective Security Officers (PSOs) ensure strict compliance with the requirements and standards outlined herein.

This SOP provides a framework of responsibilities for DHS personnel relevant to situations involving suspicious packages, letters, or other material that are reported

within the NAC, senior leaders' residences, and off-site mail facilities. Nothing in this SOP is intended to conflict with existing law, Executive Order, or Federal Regulation. This SOP complements the *Incident Command System* SOP operations.

4. AUTHORITIES

The CSO serves as the Senior Agency Official for the Department and the DO for the NAC. As such, the CSO is responsible for the administration of all DHS security programs and the day-to-day security operation of the NAC.

NOTE: This policy may be revised at the discretion of the CSO consistent with applicable law, rule, and regulation.

Authorities to provide protection and security service are contained in the following documents:

A. Public Law 107-296 (November 25, 2002) , Homeland Security Act of 2002

B. 6 U.S.C. 341 – "Under Secretary for Management"

C. 6 C.F.R. 7.10 – "Authorities of the Chief Security Officer"

D. 40 USC § 1315 , Law Enforcement Authority of the Secretary of Homeland Security for Protection of Public Property

E. Department of Homeland Security Management Directive 121-01, Chief Security Officer

F. The Facility Security Plan: An Interagency Security Committee Guide

G. Delegation 12000, Security Operations within the Department of Homeland Security

H. DHS Directive 119-01 Mail Management Program

I. Office of the Chief Security Officer (OCSO) SOP, Incident Command System (ICS), dated February 1, 2012

J. OCSO Incident Command System, Standard Operating Procedure, dated February 1, 2012

K. Deputy Secretary Approval Memo, "Nebraska Avenue Complex Security Posture," dated May 1, 2014

L. The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, August 2013

M. Memorandum of Agreement between OCSO and Federal Protective Service, dated February 11, 2015

5. DEFINITIONS

The use of mail and packages to deliver toxic substances and/or explosives is well-documented. For the purposes of this SOP, the following general definitions are provided for consideration by first responders and OCSO staff when dealing with suspicious packages, mail, or correspondence but are not intended to be all-inclusive:

A. ***Biological Weapons***: Live micro-organisms or toxins that can incapacitate or kill humans and animals. They include anthrax, plague, smallpox, tularemia, botulism, and viral hemorrhagic fever. The exact effects of the biological agent depends upon the agent used. In general, effects of biological agents is felt only after an incubation period that may last up to several weeks.

B. ***Chemical Weapons***: The term chemical weapon refers to any toxic chemical or its precursor that can cause death, injury, temporary incapacitation or sensory irritation through its chemical action. Among the commonly employed chemical agents are the following:

(1) Nerve agents. One of the better-known nerve agents is sarin. These agents attack the central nervous system and can incapacitate and/or kill.

(2) Vesicants. The most familiar of these is mustard, often referred to as mustard gas. The vesicants are so named because, among other unpleasant results, they cause blistering of the skin.

(3) Lung-damaging agents. Most prominent among these is phosgene, which is a major industrial chemical used to make chemicals and pesticides. At room temperature it is a poisonous gas.

(4) Cyanide. This is a highly lethal agent but one that is not always well suited to terrorist use because it dissipates quickly.

C. ***Explosive Weapons***: Any reactive substance that contains a great amount of potential energy that can produce an explosion if released suddenly, usually accompanied by the production of light, heat, sound, and pressure.

D. ***Nuclear Materials***: Refers to the metals uranium, plutonium, and thorium, in any form.

E. ***Senior Leader***: In DHS, defined as the Secretary, the Deputy Secretary, or anyone who reports directly to these two individuals.

6. RESPONSE LEVELS

There are two levels of response:

A. Unknown or unconfirmed presence of a threat.

This level of response incorporates all of the activities required to investigate the suspicious package, incident, or symptom, to either rule out or confirm the presence of chemical, biological, radiological, nuclear, and explosive (CBRNE) materials.

B. Confirmed presence of a threat, to include CBRNE materials.

This level incorporates all of the activities required to establish command and control in an effort to develop an Incident Action Plan to mitigate (within the capabilities of the OCSO) the release of a CBRNE, evaluate the extent of contamination, conduct life and safety operations, and initiate mutual aid and unified command as necessary.

7. ACTIVATION CONDITIONS

Upon notification of the circumstances, the Chief, Physical Security Division is generally the responsible official to activate the appropriate response required to investigate a suspicious package, incident, or symptom (suspicious or unknown substance without a package), to either rule out or confirm the presence of CBRNE materials. In the absence of the Chief, the next highest-ranking OCSO official is authorized to activate the appropriate response.

For incidents occurring on the NAC, the PSO Watch Commander activates the appropriate response, under the supervision of OCSO FPB personnel.

8. OPERATIONAL STRATEGIES INVOLVING SUSPICIOUS PACKAGES, MAIL, CORRESPONDENCE, OR OBJECTS

A. ***Threat Assessment***:

In the event intelligence information is received which suggests significant credibility should be given to a suspected or specific threat associated with a suspicious package, mail, correspondence, or object, the information is provided to the Chief, Physical Security Division and evaluated as to the response level assigned.

(1) The threat assessment should, at a minimum, include the following:

(a) Is the sender of package or substance known?

(b) Has the sender of package or substance been contacted?

(c) What was sent? Was there excessive postage?

(d) Can the package or substance be explained?

(e) Has the recipient of the package or substance received any prior threats?

(f) How and when were the threats received?

(g) What was the threat?

(h) Was there a written threat accompanying the package?

(i) Are there circumstances that could be related to the sending of a problem package such as: disgruntled or discharged employee, irate customer, labor dispute, domestic disturbance, restraining order, etc.?

(2) The assessment should consider the possibility of CBRNE device, or combination. Do not assume the threat is anthrax.

Based on the day and time of the incident, the Chief, Physical Security Division ensures that appropriate personnel are notified to report to a specific staging area for assignments.

NOTE: If there is a suspected terrorism nexus or a perceived terrorism threat, OCSO notifies the FBI's Washington Field Office at (202) 278-2000. Should the situation warrant, the subsequent investigation may be conducted jointly with the FBI (and other federal, state, and local, and U.S. Postal Inspection Service partners, if applicable).

OCSO members or PSOs who are first to encounter a suspected or specific threat associated with a suspicious package, mail, correspondence, or object, evaluate the gravity of the situation, decide on a course of action, and then set in motion the steps necessary to address the particular incident. Some events requires the utilization of additional personnel and equipment.

Based on the threat assessment and as appropriate, the DC Fire and EMS Department decontaminates individuals who have been directly exposed.

At the scene of an unusual occurrence involving a suspected or specific threat associated with a suspicious package, mail, correspondence, or object, assigned OCSO and PSO personnel assume the following specific duties and responsibilities:

(a) The protection of life and property.

(b) The investigation of crimes.

(c) The establishment of a quarantine area as needed.

(d) The maintenance of order in and around the emergency area.

(e) The prevention of unauthorized entry into the area.

(f) The control of traffic in and around the area and the maintenance of unimpeded access to, and egress from, the emergency area by authorized personnel.

(g) The safeguarding of persons and property to include:

i. Any dead and/or injured persons.

ii. Evacuated buildings.

iii. Abandoned property at the scene.

iv. Prevention of looting.

v. Public utilities, which may be at risk.

vi. Public facility and critical infrastructure security.

vii. The evacuation of unsafe buildings.

viii. The prompt notification of other governmental agencies, public utilities, and related private agencies and companies.

ix. The establishment of a command post utilizing the Incident Command System, if appropriate.

x. Cooperation with other agencies operating at the scene and coordination of activities with those agencies if

OCSO has primary responsibility.

xi. The maintenance of proper records.

xii. Safeguarding the constitutional and civil rights of all people involved.

xiii. Requesting appropriate outside agency support.

xiv. Coordinating media briefings through the Office of Public Affairs.

xv. Obtaining all necessary equipment and supplies.

xvi. Coordinating the flow of public transportation around the emergency.

xvii. Coordinating de-escalation procedures, aftermath duties, and scene release activities.

(3) OCSO FPB and PSOs arriving at the scene of a suspicious package, mail, correspondence, or object, event immediately notify the NAC Command Center of the following:

(a) The nature of the event.

(b) The exact location.

(c) The extent of damage or potential danger.

(d) The immediate assistance required.

(e) The necessary supervision required.

(f) Suspect information (if appropriate).

(g) Other pertinent information, as necessary.

B. ***Supervisory responsibilities***:

In the event of a suspicious package, mail, correspondence, or object incident, the OCSO FPB and/or PSO supervisor responds and further assesses the need for additional resources. The supervisor initiates the Incident Command System and updates the Chief, Physical Security Division. Additionally, the first supervisor on the scene assesses and coordinates the following:

(1) Request additional personnel for assignment to the scene.

(2) Specify a protected area adjacent to the scene (but within a safe distance based on the threat) as a staging area and assign an officer to be in charge of that area.

(3) Establish Incident Command, remaining cognizant of the need for a secure area.

(4) Notify NAC Command Center of the following:

(a) The location of the incident command post and the staging area.

(b) The current status of the situation.

(c) The need to move to an alternate radio channel for the operation.

(d) The need for Personal Protective Equipment to be employed by personnel on site.

(5) Establish perimeter assignments

(6) Establish an emergency response route for additional units and equipment responding to the scene.

(7) In an incident involving the NAC, notify the Federal Protective Service consistent with the existing Memorandum of Agreement with their agency.

(8) In an incident involving CBNRE, notify the Office of Health Affairs.

C. ***Incident Commander responsibilities***:

The first supervisor on the scene assumes responsibility as Incident Commander for coordinating and managing the setup and initial activation of the Incident Command System. The Chief, Physical Security Division assumes command once on the scene, at his/her discretion. This responsibility includes the following issues:

(1) Stabilization of the crime scene.

(2) Medical needs and treatment (coordinated with DC Fire and EMS Department).

(3) Temporary shelter area(s), if appropriate.

(4) Public Information area.

(5) Property recovery and disposition.

(6) Evacuations.

(7) Equipment and supplies acquisition.

(8) Assignment of task coordination, which may include:

(a) Logistics

(b) Planning

(c) Staffing

(d) Casualty Coordination

(e) Medical Treatment

(f) Transportation

(g) Staging

(9) Assessment of need to mobilize additional personnel to include off-duty and non-patrol personnel. The actual decision to mobilize additional personnel is at the discretion of the Chief, Physical Security Division in consultation with the CSO and Deputy CSO (DCSO).

9. SPECIFIC PROCEDURES FOR INCIDENTS OCCURRING ON THE NAC

**NOTE: These following procedures are followed in every incident involving the NAC. The general guidelines listed above are incorporated as appropriate and to the extent possible.**

PROCEDURES FOR SUSPICIOUS PACKAGES (suspicious package, mail, correspondence, incident, or symptom suspicious or unknown substance without a package):

A. Terminate the use of portable radios or any device transmitting radio, analog, and or digital frequencies near the location of the package.

B. Upon receipt of a call for a suspicious package, FPB law enforcement officers (LEOs) and the PSOs do the following:

(1) Respond to the scene and assess the situation;

(2) Notify your supervisor;

(3) Depending on the initial assessment, request a K9 team (if appropriate) and/or the DC Fire and EMS Department to respond;

(4) Notify Chief, Physical Security Division, who conducts an assessment to determine appropriate activation conditions;

(5) The Chief, Physical Security Division (or in his/her absence the highest-ranking official) makes a determination to activate Incident Command and/or makes a recommendation to activate the Crisis Management Team.

C. An OCSO supervisor responds to the scene and assists the FPB LEOs and the PSOs in evaluating and properly resolving the suspicious package call.

D. Until the true nature of a package is determined, efforts are made to limit access to the area of the package, to include both vehicular and pedestrian ingress and egress of the NAC if the package is located at one of those points.

E. Identify any persons exposed to the package that should be quarantined. Where applicable, air-handling systems should be turned off and doors and windows closed. It should be noted that sealed and intact packages offer little or no biohazard risk to responders.

F. To determine the credibility of a potential threat, FPB LEOs and the PSOs should attempt all reasonable efforts to determine the source and contents of the package by backtracking to its origin whenever possible.

G. Once on the scene, FPB LEOs, PSOs, and fire personnel determine if the item is suspicious in nature based on a host of information that includes but not limited to:

(1) Inappropriate or unusual labeling

(2) Excessive postage

(3) Handwritten or poorly typed addresses

(4) Misspellings of common words

(5) Strange return address or no return address

(6) Incorrect titles or title without a name

(7) Not addressed to a specific person

(8) Marked with restrictions, such as “Personal,” “Confidential,” “Hazardous Materials,” or “Do not x-ray”

(9) Marked with any threatening language

(10) Postmarked from a city or state that does not match the return address

(11) Appearance

(12) Powdery substance felt through or appearing on the package or envelope

(13) Oily stains, discolorations, or odor

(14) Lopsided or uneven envelope

(15) Excessive packaging material such as masking tape, string, etc.

(16) Other suspicious signs

(17) Excessive weight

(18) Ticking sound

(19) Protruding wires or aluminum foil

**NOTE: If a package, envelope, object, or substance appears suspicious when compared to the list above, USE CAUTION.**

H. If first responders feel that the package is suspicious in nature and could contain a CBRNE, they immediately request response by the DC Fire and EMS Department HAZMAT Unit.

(1) Unified Command establishes if appropriate, and Incident Command is instituted.

(2) The Metropolitan Police Department’s 2nd District is notified.

(3) The OCSO Supervisor makes appropriate notifications through the chain of command to the DCSO and the CSO.

(4) The CSO or his designee makes appropriate notifications to the Under Secretary for Management and the National Operations Center.

I. DC Fire and EMS Department HAZMAT Unit have primary responsibility to collect and analyze any unknown substances.

J. If a credible threat exists, the Chief, Physical Security Division, on-scene supervisor, and other personnel on the scene establish an Incident Action Plan to mitigate the hazard, to include a recommendation to evacuate of the facility, per paragraph K below (if appropriate).

K. If evacuation of the facility is appropriate, the Chief, Physical Security Division makes that determination in conjunction with the CSO, DCSO, Under Secretary for Management, and the National Operations Center.

L. If terrorism is suspected or confirmed, the Chief, Physical Security Division (or higher) ensures that the FBI is notified, but only after notifying the Under Secretary for Management of the action.

M. Any unknown substances are packaged and transported based on established protocols by DC Fire and EMS Department for qualitative and quantitative analysis.

N. If personnel on the scene feel the package is suspicious in nature and could contain explosive materials, they immediately evacuate the area to a safe distance and follow established procedures for managing BOMB THREATS/EXPLOSIVE incidents.

O. **Under no circumstances** are any suspicious packages to be transported in any OCSO vehicle unless it has been determined to be safe.

P. The CSO, in consultation with the DCSO and Chief, Physical Security Division determines who has primary responsibility for case investigation where terrorism is not confirmed or suspected.

Q. In cases where terrorism is confirmed or suspected, the CSO identifies an investigative Point of Contact to assist the agency with investigative primacy.

R. Complete all reports relating to a suspicious package situation prior to the end of the shift, unless the case is still pending, and a copy forwarded to the DCSO/CSO for review.

S. The CSO, in consultation with the DCSO and Chief, Physical Security Division, considers all the facts and circumstances associated with the incident before elevating the NAC security posture under the OCSO *Enhanced Security Measures* policy. The CSO, or his designee, advises the Under Secretary for Management of any changes to the NAC security posture relative to the incident.

T. Information resources available:

(1) DC Health Department
899 North Capitol Street, NE
Washington, DC 20002
Phone: (202) 442-5955

(2) Centers for Disease Control and Prevention
1600 Clifton Road
Atlanta, GA 30329-4027 USA
800-CDC-INFO (800-232-4636)

(3) DC Homeland Security and Emergency Management Agency
2720 Martin Luther King Jr. Ave, SE
Washington, DC 20032
Phone: (202) 727-6161

(4) Metropolitan Police Second District Station
3320 Idaho Avenue, NW
Washington, DC 20016
Phone: (202) 715-7300

(5) FBI – Washington Field Office
601 4th Street, NW
Washington, D.C. 20535
(202) 278-2000

NOTE: To report suspicious activity involving chemical, biological, or radiological materials, call (toll-free): 855-TELL-FBI or 855-835-5324.

(6) U.S. Postal Inspection Service
(877) 876-2455 (Emergency)

**Nearest office**:
10500 Little Patux Parkway, Suite 200
Columbia, MD 21044-3509

(7) DC Office of Unified Communications
2720 Martin Luther King Jr. Avenue, SE

Washington, DC 20032
Phone: (202) 730-0524

10. OFF-SITE (non-DHS related) HAZARDOUS MATERIAL OR CBRNE INCIDENTS

For off-site, non-DHS related hazardous materials incidents, OCSO monitors the incident in conjunction with the National Operations Center and assess any potential risk to the NAC.

11. PROCEDURES INVOLVING OFF-SITE SUSPICIOUS PACKAGES, LETTERS, OR OTHER MATERIALS DELIVERED TO A DHS SENIOR LEADER'S RESIDENCE

Upon notification of the circumstances that a DHS senior leader has received a suspicious package, to include mail or correspondence, the Chief, Physical Security Division in accordance with 40 U.S. Code § 1315 is generally the responsible official to activate the appropriate response required to investigate the matter. In the absence of the Chief, the next highest-ranking OCSO official is authorized to activate the appropriate response.

There are generally <u>two</u> levels of response:

A. <u>Unknown</u> or <u>unconfirmed</u> presence of a threat. The senior leader is advised to:

(1) NOT OPEN OR DISTURB THE LETTER OR PACKAGE;

(2) Call 911 (local authorities) if the circumstances warrant;

(3) NOT put the letter or package in his/her car or bring it to work; and

(4) Contact the NAC Command Center at: (202) 282-9700.

NOTE: The NAC Command Center supervisor contacts the OCSO FPB, who in turn notifies the Chief, Physical Security Division. The Chief assess the facts and circumstances and determine if a response to the senior leader's residence is warranted to investigate the suspicious package, mail, or correspondence. This level of response incorporates all of the activities required to investigate the potential threat to the senior leader and the suspicious package. If there is ANY doubt about the potential presence of CBRNE materials, OCSO FPB personnel do not take custody of the package. That responsibility rests with local authorities.

B. The <u>suspected</u> OR <u>confirmed</u> presence of a threat, to include CBRNE materials, the senior leader is advised to:

(1) NOT OPEN OR DISTURB THE LETTER OR PACKAGE;

(2) NOT CHANGE OR TOUCH ANYTHING, including using the phone, turning lights, computers, etc. on/off;

(3) Immediately call 911 (local authorities) from a safe location (500 feet) away from the package;

(4) Verbally notify others in the area of the situation;

(5) NOT put the letter or package in his/her car or bring it to work;

(6) NOT put the item in water, or a confined space such as a desk drawer or filing cabinet;

(7) Get everyone out of the room; direct people to a designated area away from the package to await further instructions;

(8) Evacuate to an established safe perimeter which may be up to 500 feet; the approximate length of two football fields;

(9) Contact the US Post Office's Dangerous Mail Investigations Duty Inspector from a safe location away from the package at: (202) 631-0588 or (877) 696-5322.

(10) Contact the NAC Command Center at (202) 282-9700.

(11) Assist in the investigation with appropriate authorities.

(12) Contact the FBI LNO to DHS at 202-282-8154

NOTE: The NAC Security Desk supervisor contacts the OCSO FPB, who in turn notifies the Chief, Physical Security Division. The Chief assess the facts and circumstances and determine if a response to the senior leader's residence is warranted to assist local authorities with the suspicious package, mail, or correspondence and to act as a POC for the Department. This level of response incorporates all of the activities required to determine departmental actions necessary to protect the senior leader going forward.

The CSO is assigned the investigative case responsibility for the matter. For investigations that fall within the jurisdiction of another federal agency, the CSO assigns an OCSO POC for coordination purposes.

In matters involving the jurisdiction of OCSO, the CSO provides regular investigative updates to the Under Secretary for Management and the affected

DHS senior leader.

## 12. PROCEDURES INVOLVING OFF-SITE SUSPICIOUS PACKAGES, LETTERS, OR OTHER MATERIALS DELIVERED TO DHS OFF-SITE MAIL FACILITY

Upon notification of the circumstances that the Consolidated Remote Delivery Site has received a suspicious package, to include mail or correspondence, the Chief, Physical Security Division is generally the responsible official to activate the appropriate response required to investigate the matter. In the absence of the Chief, the next highest-ranking OCSO official is authorized to activate the appropriate response.

## 13. REPORTING PROCEDURES

Every incident involving a suspicious package, mail, or correspondence is documented by the assigned OCSO FPB or ISID investigator in a Report of Investigation (ROI), which is reviewed and approved by a supervisor. Each ROI receives the appropriate classification markings and is forwarded to the appropriate officials for review and subsequent forwarding to the appropriate agencies when applicable.

The CSO, through the Under Secretary for Management, keeps any affected senior leader apprised of investigative efforts regarding their cases.