Section-04 Security	OP-040119	Page: 1	Effective Date: 08/23/2021
Intelligence	**ACA Standards: 2-CO-1F-07, 5-ACI-1A-20, 5-ACI-1F-03, 5-ACI-1F-08**		
Scott Crow, Director **Oklahoma Department of Corrections**		**Signature on File**	

Intelligence

The mission of the office of the Inspector General (OIG) Security Threats Intelligence (STI) division is to collect, assess and analyze information and produce intelligence regarding threat and/or criminal activity within the Oklahoma Department of Corrections (ODOC) to ensure the safety and security of all employees, visitors and inmates.

The OIG will collect information and produce intelligence regarding threat and/or criminal activity generated within ODOC, which may be projected toward outside individuals and communities. The OIG, in collaboration with ODOC employees and contract facility staff, will identify security threat groups (STG) and their members within the agency to assist in the mitigation of the threats they pose.

The OIG recognizes that certain criminal activities including, but not limited to, gang crimes and drug trafficking, often involve a degree of regular coordination and may involve a large number of participants over a broad geographical area. It is the policy of the OIG to collect and share relevant information with other law enforcement entities while respecting the privacy and legal rights of the public. (5-ACI-1F-08)

I. Definitions

A. Criminal Intelligence

Intelligence which has been evaluated and determined to be relevant to

the identification of a person or persons and/or organization involved in criminal activity.

B. Criminal Intelligence System

A record keeping system that receives, stores, exchanges and/or disseminates information that has been evaluated and determined to be relevant to the identification of a criminal organization or enterprise.

C. Intelligence

Information or data which has been analyzed and evaluated and is determined to be relevant to ODOC security or criminal activity.

D. Security Threat Group

Any group, organization, or association of three or more individuals who possess common characteristics which serve to distinguish them from other individuals or groups, and who have been determined to be acting together, and posing a threat or potential threat to the safety or security of staff, other inmates, ODOC institutions, or outside communities.

II. Data Collection

The following procedures will be utilized by OIG to ensure information is collected, evaluated and disseminated to the appropriate staff members and related criminal justice/human service agencies in order to meet the mission of ODOC. (2-CO-1F-07, 5-ACI-1F-08)

A. Use of Data

STI will collect information in order to identify threats, criminal activity, and suspicious activities that appear to be related to threats or criminal activities, which may involve STG or others who operate within ODOC and/or those who may threaten outside communities.

1. Criminal Intelligence System

The person designated by the Inspector General (IG) will be responsible for maintaining each criminal intelligence system controlled by the OIG. The designated person will ensure the following:

a. OIG employees using such system are trained in the operation of the system;

b. User access to the criminal intelligence system is reviewed and audited at least annually; and

c. All security system issues are addressed.

2. System Entries

It is the responsibility of the IG or their designee to approve the entry of any information into an authorized criminal intelligence system. All supporting documentation for an entry will be retained in criminal intelligence files. (5-ACI-1F-03 b#2, b#3)

B. Sources

The OIG will collect information based on the collection requirements allowed by state and federal statutes and not prohibited by agency policy; this may include STG information, communications or storage device exploitation, ODOC or contract databases, external law enforcement or commercial databases, open source information, social media and human sources. (5-ACI-1F-03 b#1)

Resources used to gather and/or collect intelligence may include, but are not limited to, the following:

1. Reports;

2. Other law enforcement or correctional personnel;

3. Anonymous tips;

4. Informants; and/or

5. Media.

C. Reporting

Each ODOC/contract facility, the administrator of Institutions and the chief administrator of Community Corrections and Contract Services will report the following information via the OIG's email account (sti@doc.ok.gov) or a designated (see Section III, part A of this procedure) OIG agent or analyst. Once received at STI, the information will be assessed to determine if any immediate action is required or if the information will be retained by the OIG for future intelligence purposes.

The following information will be reported/provided to the OIG for the purposes of intelligence collection:

1. Reportable incidents as defined in OP-050108 entitled "Use of Force Standards and Reportable Incidents."

2. All Incident/Staff Reports (OP-050109, Attachment A) entitled "Reporting of Incidents" and/or other reports associated with the

following potential threat and/or criminal activity incidents listed below: (5-ACI-1F-03 b#1)

a. Bomb threats or explosions on or near ODOC properties that may have been intended for ODOC facilities;

b. Incidents which pose or could pose an ongoing threat to physical, electronic, or computerized institutional security. (This includes exposure of electronic or computerized systems to viruses or other electronic threats or exposure of air-gapped computer systems to internal or external networks or unapproved hardware or software.) (5-ACI-1F-03 b#1, b#2, b#3);

c. Discovered, attempted, or suspected contraband drop, to include those seen in person, discovered on security footage, learned about through other sources or any information regarding future contraband drops;

d. Mail, either incoming or outgoing, inmate-to-inmate notes/correspondence (e.g., “kites”) or other items of a suspicious nature that contain writings/information regarding threats, criminal activity, codes/ciphers, or other writings of suspicious nature. Mail may be in the form of physical documents or electronic (e.g., email).

e. Sightings of unmanned aircraft systems (UAS’s), also known as drones, above or near ODOC or contract facilities, including any UAS’s recovered at or near ODOC or contract facilities. These incidents shall be reported immediately to the administrators of Institutions, who will be responsible for contacting STI. Actions should be taken to preserve the scene in accordance with OP-050601 entitled “Unmanned Vehicles”;

f. Information on any STG members, associates, or suspected members, which is or may be related to threat or criminal activity;

g. Arrests or criminal charges against ODOC/contract facility employees that are drug related or may be related to criminal activity within ODOC or contract facilities;

h. Threats, retaliation, retribution, or harm against ODOC/contract facility employees or the families of;

i. Attempted blackmail, coercion, or bribery of a ODOC/contract facility employee or family member(s) of an employee by an inmate or a family member of an inmate;

j. Staff member(s) that have been targeted for recruitment by inmates;

k. Known or suspected membership of any ODOC employee in any recognized STG or other criminal organization;

l. The seizure of contraband electronic devices (cellular telephones, etc.), known or suspected to have a nexus to an STG group or member, contraband, drug trafficking, threat information or other criminal information;

m. Information regarding an inmate's or an ODOC employee's or contract facility staff member's involvement in an international drug trafficking organization or cartel; or any other information which may be related to a drug trafficking organization or cartel;

n. Information received from outside law enforcement regarding ongoing criminal activity or threat information within ODOC facilities or contract facilities responsible for housing ODOC inmates;

o. Information developed by facilities or other offices within ODOC regarding inappropriate or possible criminal activity by an ODOC staff member;

p. Information pertaining to a staff member that is terminated for a cause related to drugs, contraband, or other illegal activity, or staff member who resigns under suspicion or investigation of drugs, contraband, or other illegal activity;

q. Suspicious inmate financial or inmate communication system activity, which may be related to contraband, drug trafficking, threat, or other illegal activity;

r. Known aliases, nicknames, or "yard names" of inmates;

s. Known terminology, slang, or code words used by inmates to covertly discuss contraband, drug trafficking, threat, or other illegal activity;

t. Known nicknames, "yard names", terminology, slang, or code words used by inmates to describe an individual correctional officer or ODOC staff member, or correctional officers or ODOC staff members in general; and

u. Information, which is related to or may be related to

terrorism, terrorism related recruitment, terrorism related radicalization or terroristic threats.

III. Security Threat Groups (STG)

A. Each ODOC and contract facility will have an assigned OIG intelligence agent and a criminal interdiction Agent who will work with facility staff members to assist in the identification of STGs, members, suspected members, and associates, as well as any other threats or criminal activity. Additionally, the agents will assist in identifying any projected threat to outside individuals or communities. The OIG will:

1. Assist in the further development and training of STG officers in all ODOC and contract facilities;

2. Conduct a quarterly intelligence meeting with facility STG officers and other law enforcement agencies;

3. Provide training opportunities to new corrections employees and other staff as appropriate regarding the identification of STG's. The OIG will also provide STG training to outside law enforcement agencies upon request and as approved by the Inspector General; and

4. Enter data on identified, validated, or suspected STG members and associates into the Offender Management System (OMS) and into the intelligence and investigative records management system (IIRMS). Other threats and/or criminal activity will be entered into (IIRMS). Staff will enter any known and/or suspected terrorist affiliation, if appropriate, into (IIRMS). (5-ACI-1A-20 b#1, b#2)

B. Inmates will be assessed and identified as validated members, suspected members, or associates of an STG based upon reliable, documented information or history of gang or terrorist activity while confined or in the community. Suspected members and associates have met one or more of the validation criteria listed in the "Security Threat Group STG Validation Form" (Attachment A, attached), but have not acquired enough points to be considered validated members.(5-ACI-1A-20 b#1)

1. If one of the five items apply under the "Security Threat Group" section on the "Incident/Staff Report" (OP-050109, Attachment A), or any other information is obtained which indicates gang activity or gang involvement, a "Security Threat Group (STG) Validation Form" (Attachment A, attached) will be completed by the chief of Security or designee and forwarded to the STI.

STI staff will evaluate the information contained in the "Security Threat Group (STG) Validation Form" (Attachment A, attached) and enter the information into OMS and the OIG database.

2. In the event an inmate admits gang membership, a "Security Threat Group Intelligence Admittance Form" (Attachment B, attached) and an "Initial Security Threat Group Assessment Questionnaire" (Attachment C, attached) will be completed by the chief of Security and forwarded to the STI.

3. An inmate who was previously assessed and identified as a validated member of a STG may be officially designated as "validated-inactive", with the approval of the Inspector General or designee following the completion of the below process:

   a. An inmate may submit a "Request to Staff" form (OP-090124, DOC 090124D) to have their STG assessment reviewed and their status officially changed to "inactive."

   b. The chief of security will review the inmate request and complete the "Security Threat Group Membership Status Review Form" (Attachment D, attached). If the facility staff member determines the inmate does not meet all the listed criteria, the request will be denied by the facility.

   c. If the inmate meets the following criteria, the "Security Threat Group Membership Status Review Form" (Attachment D, attached) will be forwarded to the OIG for review:

      (1) Inmate denies active gang membership;

      (2) In the past 5 years, inmate has not been involved in a reportable incident related to contraband introduction, inmate assaults or fights, assaults on staff, or other STG related activity, unless as a victim or witness;

      (3) Inmate has no active Class X misconducts; and

      (4) Inmate does not regularly associate with active, validated STG members except as a result of housing assignment.

   d. The OIG will review the completed "Security Threat Group Membership Status Review Form" (Attachment D, attached), attach any additional relevant information, and forward to the Inspector General or designee for approval or denial.

   e. Pre-existing tattoos will not prevent an inmate from obtaining validated-inactive status. While certain tattoos or tattoo removal or covering may be indicative of gang activity or inactivity, ODOC does not condone or encourage tattooing or tattoo removal by inmates. Any STG related tattoos

acquired by the inmate after requesting validated-inactive status may result in the inactive status being revoked.

f. The requesting facility will be notified of the results of the STG Membership Status Review via Memorandum from the OIG. Inmates who receive approval from the IG will have their membership status updated to validated-inactive.

g. Validated-inactive STG members will continue to be tracked by the OIG.

h. Any ODOC or contract facility staff member who becomes aware of a validated-inactive STG member who no longer meets the criteria to be considered validated-inactive will complete the "Revocation of Inactive STG Membership Status" form (Attachment E, attached). The staff member will submit the form and supporting documentation to the chief of Security for review. If the chief of security agrees with the initial assessment, they will forward the "Revocation of Inactive STG Membership Status" form (Attachment E, attached) and supporting documentation to the OIG for review. The IG or designee will determine whether or not to revoke the inmate's validated-inactive status.

i. If an inmate's validated-inactive status is revoked, they will once again be considered a validated member and will not be eligible to be reconsidered for validated-inactive status for a period of 10 years.

j. If during the STG Membership Status Review, or any other review of an inmate's STG information, the OIG determines an inmate was validated in error, or the OIG does not have documentation to support the validation, the inmate will be removed from the STG list. In the event an inmate is removed from the STG, the facility housing the inmate will be notified by memorandum from the OIG.

4. Any security protocols or lockdowns, based on STG membership status, will be determined by the division of Institutions or the facility head.

a. The four membership statuses: validated member, suspected member, associate, and validated-inactive, may be considered independently at the discretion of the division of Institutions or the facility head.

C. The OIG will collect information on suspected and/or emerging groups for validation as ODOC recognized STGs. OIG employees will present information and intelligence regarding suspected or emerging groups

being considered for validation to the Inspector General or their designee in the form of a threat assessment. Suspected or emerging groups may be designated as Watch Groups during the information collection process.

1. The threat assessment shall contain, but is not limited to, the following information:

   a. Name, ODOC number, and current location of suspected member(s);

   b. Group identifying characteristics;

   c. Criminal and/or disruptive activity by suspected group member(s);

   d. Group literature, symbolism, or by-laws;

   e. Information received from other criminal justice agencies; and

   f. Group designation as a gang, criminal organization, or STG by other criminal justice agencies.

2. The Inspector General or their designee will review the threat assessment of any group being considered for validation as a recognized STG. Following consultation with the agency director, chief of Operations and General Counsel, the Inspector General or their designee will approve or deny the designation of the group as an ODOC recognized STG. A denial of designation of a group as an ODOC recognized STG does not prevent future threat assessments of the same group. All group threat assessments and supporting documentation will be maintained by STI.

D. The Inspector General or their designee will contact the Federal Bureau of Investigation's Joint Terrorism Task Force (JTTF) when information is reported/gathered regarding incidents, events, or threats which appear to have possible terrorism connection. (5-ACI-1A-20 b#2, b#3)

1. A list of inmates involved with known terrorist ideologies and/or membership with terrorist organizations will be maintained by STI and shared with authorities as appropriate. (5-ACI-1A-20 b#1)

2. Consultation with the JTTF will occur at least semi-annually, to share intelligence gathered. (5-ACI-1A-20)

IV. Electronic Devices

A. The OIG will attempt to examine electronic devices such as contraband cellular telephones, as appropriate, to gather information, or identify

potential threats and/or criminal activity.

1. All contraband electronic devices will be submitted to the OIG.

2. The Chain of Custody on the "Contraband/Evidence Tag" (OP-040109, Attachment A), must be completed and submitted with each electronic device submitted to the OIG.

3. If an electronic device is known or believed to contain information regarding contraband introduction, illegal drugs or other criminal activity, PREA information, STG information, or threat information, that information will be noted on the "Contraband/Evidence Tag."

4. Weapons, drugs, tobacco and all other miscellaneous contraband items must be separated from electronic devices prior to submitting the electronic devices to the OIG.

V. Reports

Reports will be prepared by the OIG as outlined below and distributed to the appropriate ODOC leadership, staff and/or outside law enforcement agencies with a right to know and need to know, as noted.

A. Monthly Intelligence Report

The OIG will distribute a "Monthly Intelligence Report," which summarizes STG incidents and STG validations collected from the previous month, as well as current officer awareness information and a comprehensive list of known/suspected STG members and/or associates currently incarcerated or under supervision as appropriate to appropriate senior staff.

B. Other Reports

The OIG will prepare intelligence notes and other intelligence or threat related reports as deemed appropriate and disseminate as determined appropriate by the IG or designee.

VI. References

28 CFR Part 23

OAC 375:35-1-2 and OAC 375:35-3-2.

OAC 375:35-3-3, OAC 375:35-3-4

OP-040109 entitled "Control of Contraband and Physical Evidence"

OP-050108 entitled "Use of Force Standards and Reportable Incidents"

OP-050109 entitled “Reporting of Incidents”

OP-050601 entitled “Unmanned Vehicles”

VII. Action

The Inspector General is responsible for compliance with this procedure and for the annual review and revisions.

Any exception to this procedure will require prior written approval from the agency director.

This procedure is effective as indicated.

Replaced: Operations Memorandum No. OP-040119 “Intelligence” dated July 13, 2020

Distribution: Policy and Operations Manual
Agency Website

Referenced Forms	Title	Location
Attachment A	“Contraband/Evidence Tag”	OP-040109
Attachment H	“Initial Notification Checklist”	OP-050108
Attachment A	“Incident/Staff Report”	OP-050109

Attachments	Title	Location
Attachment A	“Security Threat Group (STG) Validation Form”	Attached
Attachment B	“Security Threat Group Intelligence Admittance Form”	Attached
Attachment C	“Initial Security Threat Group Assessment Questionnaire”	Attached
Attachment D	“Membership Status Review Form”	Attached
Attachment E	“Revocation of Inactive STG Membership Status”	Attached