NG-J2 White Paper
The Role of National Guard Intelligence During Civil Disturbances

1. Introduction and Purpose:

Recent large-scale civil disturbances in two states led the respective governors to mobilize state National Guard (NG) forces. These incidents raised questions and concerns about the appropriate and effective use of NG intelligence capabilities to support domestic civil disturbance operations. Domestic missions are no different from overseas missions in that a key requirement for mission success is situational awareness (SA)—leaders and commanders at all levels must be aware of the situation on the ground and have a deep understanding of the operational environment in which their forces are operating and the inherent threats faced in that environment. Overseas, where the threat is by definition foreign, the intelligence component provides the preponderance of threat data. Domestically, defining threat information may entail the collection of information concerning U.S. persons. By law, the military and civilian intelligence components face constraints in the manner they may lawfully collect, disseminate, and retain such information.

Senior leaders at both National Guard Bureau (NGB) and the Joint Force Headquarters State (JFHQs-State) have requested clarification concerning the lawful use of NG intelligence capabilities (personnel and equipment) in such contingencies. This White Paper provides NG leaders an executive summary of the appropriate use of NG intelligence capabilities during civil disturbances, addresses the related legal and regulatory constraints and provides recommendations to improve NG preparedness for the use of intelligence resources in future civil disturbances. This paper also provides a broad overview of the rules and authorities for the collection of all categories of information for SA in the domestic arena.

2. Background:

NG domestic intelligence activities must be conducted within the strict boundaries set by Intelligence Oversight (IO) Directives, Service IO guidance, privacy laws, and the Constitution. Simply put, Department of Defense (DOD) Intelligence activities are limited to collection against foreign intelligence and counterintelligence threats unless specifically approved by the Secretary of Defense (SECDEF). During domestic operations (DOMOPS), the NG routinely conducts Incident Awareness and Assessment (IAA) operations designed to characterize the operational environment in order to satisfy critical information requirements for commanders and other response leaders. IAA is an intelligence-centric operation and if done effectively, it can prove decisive. When IAA operations occur, commanders must understand that intelligence organizations and capabilities may not target or intentionally collect information on U.S. Persons. Any domestic criminal or terrorist information incidentally collected by the NG intelligence component must be handed over to J-34 or law enforcement channels. Commanders require a firm understanding of the constraints imposed on intelligence personnel and organizations by DOD 5240.1-R, *Procedures Governing the Activities of DoD Intelligence Components that Affect U.S. Persons,* as well as the constraints imposed on all non-intelligence activities by DOD Directive (DODD) 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense.*

Before discussing the rules concerning the collection, retention and dissemination of information within the homeland, it is important to understand that there are two distinct groups of Guardsmen who collect information. Each group must operate according to its own authorities and rules. The first group is generally composed of Intelligence personnel and equipment assigned to the J2, A2 and G2; the second group, the National Guard at large (non-intelligence component) to include Domestic Operations (J3/G3/A3); Command, Control, Communications and Computers (J6/G6/A6); and Military Police and Security Forces personnel. Because each has its own authorities and rules, it is imperative that commanders and leaders direct their requests for information to the appropriate group.

3. Definitions:

A. Federal Intelligence Equipment vs. Non-intelligence Equipment: Simply stated, Federal intelligence equipment is equipment that has been purchased with Military Intelligence Program (MIP) or National Intelligence Program (NIP) monies. Examples of Federal intelligence equipment include the Raven and Shadow Unmanned Aircraft Systems (UAS), Joint Worldwide Intelligence Communications System (JWICS), MC-12 aircraft, and Distributed Common Ground Station (DCGS) weapon system. State Governors, as commanders-in-chief, can directly access and utilize the NG's federally assigned aircraft, vehicles and other general purpose equipment (i.e., non-intelligence equipment) so long as the Federal government is reimbursed for the use of fungible equipment and supplies. SECDEF approval, however, is required to use Federal intelligence equipment for any purpose other than foreign intelligence or counterintelligence (i.e., its Title 10 mission or Title 32 training to prepare for that Title 10 mission).

B. National Guard Intelligence Component: NGB, Title 32 NG JFHQ-S, and Title 32 NG intelligence units and staff organizations and non-intelligence organizations that perform intelligence or intelligence-related activities.

C. U.S. Person: A U.S. citizen, born in the U.S. or naturalized; an alien known by the DOD intelligence component concerned to be a permanent resident alien; an unincorporated association substantially composed of U.S. citizens or permanent resident aliens; or a corporation incorporated in the U.S., unless it is directed and controlled by a foreign government or governments.

4. Domestic Information Collection – Category of Collectors:

A. Intelligence Personnel (J2, G2 and A2) and Equipment: Intelligence personnel in Title 10 or Title 32 status and the Federal intelligence equipment they employ are subject to the IO rules contained in DOD 5240.1-R and Chief National Guard Bureau Instruction (CNGBI) 2000.01, *National Guard Intelligence Activities*, and its accompanying manual (CNGBM 2000.01). Information concerning U.S. Persons may only be collected by Intelligence Personnel and equipment if it is necessary to carry out an authorized mission and falls within an approved category of information as listed in DOD 5240.1-R. By law, the only authorized missions for Title 10 Intelligence personnel and equipment and Title 32 intelligence personnel training for their Title 10 mission are foreign intelligence and counterintelligence. SECDEF approval is required to use Title 10 intelligence personnel and Federal intelligence equipment for any use other than their Title 10 (Foreign Intelligence or Counterintelligence) mission.

During DOMOPS, Title 32 NG intelligence personnel may leverage their Title 32 training Mission Essential Task Lists (METL) tasks and non-intelligence equipment to provide SA of the operational environment so long as it is not for the purpose of targeting, or collecting on, any specific U.S. Persons. They may monitor foreign threats to the NG/DOD and all-hazards threats (natural and manmade disasters and incidents). This includes lines of communication analysis; key and critical infrastructure status and vulnerabilities; movements of large crowds (not specific U.S. Persons); the erection of street barriers; the location of citizens or incident responders in distress (consent of the U.S. Person is implied in these circumstances); geographical location of the large-scale destruction of property (e.g., arson and looting); attempts by foreign terrorist organizations to exploit vulnerabilities during DOMOPS, even when foreign actors have played no role in the incident; and the effects of weather and terrain on planning and operations. Any domestic criminal or terrorist information concerning specific U.S. persons incidentally collected by NG intelligence personnel in the routine performance of their duties must be handed over to the J-34 or law enforcement officials. Based on their understanding of the operational environment, NG intelligence personnel should play a key role in the formulation of Priority Intelligence Requirements, Commander's Critical Information Requirements, and Friendly Forces Information Requirements.

Governors may also leverage the military intelligence (MI) skills of NG intelligence personnel under State Active Duty (SAD) with non-Federal Intelligence equipment or State equipment. While they are not subject to the DOD IO or DODD 5200.27 rules in a SAD status, all NG personnel are subject to the provisions of State law, to include Privacy Laws when it comes to collecting, using, retaining and disseminating U.S. Persons information. Consultation with the State Judge Advocate is highly recommended. Federal intelligence equipment and facilities may only be used in a SAD status with SECDEF approval.

B. National Guard "At Large" (Non-Intelligence Personnel): Non-intelligence personnel are subject to the rules contained in DODD 5200.27 and CNGBI 2400.00. Non-intelligence personnel may collect information concerning Non-DOD-Affiliated (NDA) Persons (U.S. Persons and foreign nationals) if it is necessary to carry out one of three authorized missions:

1. Protection of NG/DOD functions and property (mission, personnel, equipment and facilities)
2. Personnel security
3. Operations related to civil disturbance

During DOMOPS, NG non-intelligence personnel may leverage their Title 32 training METL tasks and non-intelligence equipment to provide SA of criminal and domestic threat emanating from U.S. Persons and foreign nationals (NDA-affiliated persons) to the NG and DOD.

5. Domestic Information Collection – Activities/Missions:

A. IAA: IO rules and other domestic imagery policy universally apply to the collection, use, retention and dissemination of domestic imagery and other geospatial information for SA purposes, known as IAA. The imagery and geospatial information must be necessary to carry out an authorized mission and must not be for the purpose of targeting any specific U.S. Person without consent.

The National Geospatial Intelligence Agency (NGA) is responsible for satellite (commercial, tactical and national) imagery collection policy. Higher-level approval is not required for the use of domestic commercial satellite imagery and other geospatial information. However, its use must be necessary for carrying out a valid mission, and the J2/G2/A2 must maintain on file an internal Memorandum for Record certifying its proper use, or that IO rules are being followed.

The Defense Intelligence Agency (DIA) is responsible for airborne (manned and unmanned) imagery collection policy, and mandates that an approved Proper Use Memorandum (PUM) be on file prior to any domestic airborne imagery collection mission.

Imagery collected during DOMOPS may be provided/shared with other DOD entities (to include NGB) and civil authorities (to include state authorities) as required based on validated need. Civil authorities are authorized to disclose or release selected Unclassified-For Official Use Only (FOUO) imagery products to participating or affected private citizens when the disclosure/release would prevent injury or loss of life and/or facilitate disaster mitigation and recovery efforts. Specific imagery products may be released to the U.S. media during senior official press conferences to provide visual depiction of disaster area status and disaster response activities. Incidentally collected images that indicate a crime has been or is being committed may be passed to law enforcement officials. However, altering the course of an airborne sensor from an approved IAA collection track to loiter over suspected criminal activities would no longer be incidental collection and is not authorized.

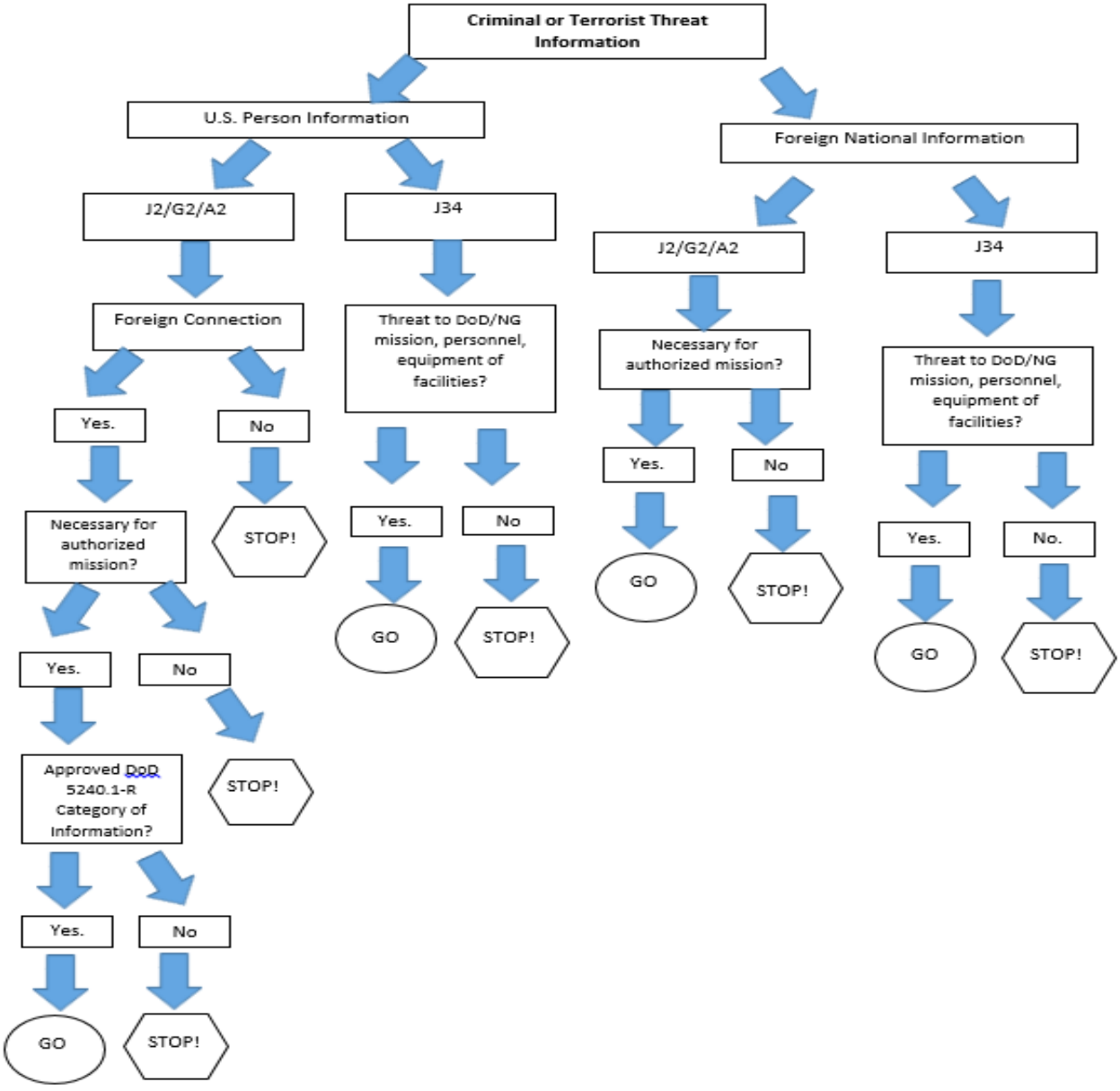
Important Caveat! The discussion above of IAA support during DOMOPS presumes that the intelligence organizations and non-intelligence assets or SECDEF-approved intelligence assets are supporting a military commander deployed as part of the interagency incident response team. If intelligence personnel or assets are supporting law enforcement organizations directly for any purpose, then the supported law enforcement agency (LEA) must request authorization from the SECDEF under Procedure 12 of DOD 5240.1-R. Information and analysis produced by intelligence personnel and assets for a supported LEA under a SECDEF-approved Procedure 12 request must be turned over entirely to that LEA and may not be retained on DOD systems.

B. Cyber: Command, Control, Communications and Computers (J6/G6/A6) personnel will work to ensure the integrity of NG/DOD networks and systems and may report on any activity that threatens DOD Networks. The J34 will collect information and report on the domestic criminal threat to NG and DOD networks and systems. The J2 will collect and report information on foreign threats to NG and DOD networks and systems.

C. Unmanned Aircraft Systems (UAS)/Remotely Piloted Aircraft (RPA): The use of UAS/RPA for DOMOPS requires SECDEF approval. It is also subject to IO and domestic imagery policy, and requires an approved PUM. This includes the use of UAS/RPA for Public Affairs Office (PAO) and Weapons of Mass Destruction-Civil Support Teams (WMD-CST) response purposes. The use of UAS/RPA for immediate response is not authorized; however, there is a Search and Rescue (SAR) exception by which the U.S. Northern Command (NORTHCOM) or U.S. Pacific Command commanders may authorize the use of UAS/RPA for SAR purposes involving distress and potential loss of life if and when the Air Force Rescue Coordination Center (AFRCC), Alaska Rescue Coordination Center (AKRCC), or Joint Rescue Coordination Center (JRCC)-Pacific determine that

UAS/RPA would be the best platform to assist in the SAR mission and that its use would not interfere with the primary military duties of the UAS/RPA unit concerned.

D. Social Media: Large volumes of useful information can be obtained via social media during domestic response. NG personnel may monitor social media using organizational accounts to meet an increased need for overall SA. The J3 may report on the domestic and criminal threat. The J2 may report on the all-hazards and foreign threats. The PAO may use social media to assess and report on the public sentiment, both to develop strategic communications for CNGB, and to maintain conversancy with public media trends and directions.



6. Identification of U.S. Persons Information:

Whether originating from intelligence or non-intelligence personnel, all U.S. persons information collected, retained and disseminated must be clearly identified as such in all products (e.g., e-mails, reports, and briefings) in accordance with DOD 5240.1-R and DODD 5200.27. E-mails and the front cover of reports and briefings with U.S. Persons information will carry the banner:

"FOUO - Information provided contains U.S. persons information. DODD 5200.27 and DOD 5240.1-R must be followed. Only distribute to those with the appropriate clearance and need to know."

Additionally, the first time a U.S. person is mentioned in an e-mail, report or briefing, it must be identified as "USPER".

7. Summary and Way Ahead:

IAA can be a decisive force multiplier during domestic response operations. As such, the NG intelligence enterprise must maintain focus on mastery of this complex mission set. That mastery will only be realized through training and education efforts. Training must focus on intelligence personnel, operational commanders and response leaders. The NG J2 Joint IAA Team (JIT) Course has trained over 500 personnel on how to legally and effectively employ intelligence capabilities during all-hazard DOMOPS. In addition, NG-J2 has conducted MI-focused staff assistance visits to 53 of the 54 States and Territories to ensure a thorough understanding of IO requirements. J2 must continue to educate senior leaders concerning the critical contribution intelligence can provide so they are knowledgeable and confident concerning the proper use of intelligence assets during domestic contingencies.

Similarly, NGB senior leaders should ensure a program is implemented to train non-intelligence personnel on the provisions of DODD 5200.27. Finally, it is important that the J2, J3, and Public Affairs establish policy on appropriate monitoring of social media during DOMOPS given the constraints upon use of U.S. Person information by both intelligence and non-intelligence elements.

8. References:

DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect U.S. Persons*
CNGBI 2000.01, *National Guard Intelligence Activities*
CNGBM 2000.01, *National Guard Intelligence Activities*
DODD 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense*
CNGBI 2400.00, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense*

Prepared by:
Mr. Terry Quist, Mrs. Gisele Singleton,
Col Gregory Keetch

Approved by:
MG Reynold Hoover
Director, NG-J2