APRIL 27, 2025

# STATE MACHINES

# STATE MACHINE STRUCTURE

| Parameter | Meaning | Example |
|---|---|---|
| Current Phase | The phase of the TCPED or F2T2EA cycle where the activity is happening. | Find, Fix, Track, Target, Engage, Assess |
| Current Activity | The specific task or process currently being performed. | Configure SAR payload settings, Prioritize tasking of sensors |
| Trigger | The event or condition that causes the transition from the current activity to the next. | Mission Tasking Received, Payload Configuration Complete |
| Next Activity | The task or process that occurs immediately after the current activity. | Prioritize tasking, Secure command and data links |
| Responsible Role | The team, organization, or individual role accountable for performing the activity. | Payload Operations Specialists, Cybersecurity Engineers |
| Intelligence Needed | The specific data, reports, or intel required to successfully perform the activity. | AOI details, PIRs, Historical SAR datasets |
| Hardware/Support | The technical tools, systems, or platforms required to execute the activity. | Wide-area imaging system, Secure Operations Center |
| Location/Timing | Where and when the activity is performed (physical or logical locations and phase timing). | Ground Control Station, Pre-Collection, Continuous Operations |
| Event Priority | How critical the activity is to mission success (affects urgency and allowed delays). | High, Medium, Critical |
| Transition Type | Whether the transition happens automatically or needs human/manual approval. | Automatic, Commander Approval, Manual |
| Failure Recovery Path | The fallback plan or recovery action if the activity fails. | Retry Configuration, Fallback to Default Prioritization |
| Authority Approval Required | Whether someone (like a commander or director) must explicitly approve before proceeding. | Yes, No |
| Data Classification Level | The security classification of the information being used or generated during the activity. | Secret, Top Secret |
| Max Allowed Delay | The maximum amount of time allowed before the activity must complete to stay within mission parameters. | Immediate, 1 Hour, 6 Hours |
| Triggering System | The system that senses, reports, or logs the trigger event that initiates the activity. | C4ISR Tasking Portal, COMSEC Authentication System |
| Data Dependency | Whether the activity depends on incoming data outputs from other systems or activities. | Mission tasking order, Encryption Integrity Reports |
| Risk Level | An assessment of how risky this activity is to mission success if something goes wrong. | Medium, High, Very High |
| External Coordination Needed | Whether coordination with external agencies, partners, or systems is necessary for successful completion of the activity. | Yes, No |

# DOD KILL CHAIN: F2T2EA - STATE MACHINES

## Find

1. In the Find phase, when a Mission Tasking is received, Payload Operations Specialists at the Ground Control Station will configure SAR payload settings using the wide-area imaging system based on AOI details and imaging mode requirements. This transition is automatic, has a high event priority, and if a failure occurs, they will retry configuration/uplink. No authority approval is required, the data classification is Secret, and the maximum allowed delay is 1 hour.
2. Following the payload configuration, once Payload Configuration is complete, Collection Managers and Mission Managers will prioritize the tasking of spacecraft sensors at the Command and Control Node. They use PIRs and Asset Availability Reports to optimize priorities. Approval is required for this transition, the event priority is high, and fallback will be to default prioritization if it fails. Data is classified as Top Secret, and action must be completed within 2 hours.
3. After prioritization, when Tasking is prioritized, Cybersecurity Engineers and Cyber Warfare Specialists will secure command and data links at the Secure Operations Center, using network communication pathways and encryption keys. This action is automatic, carries a critical event priority, and if a failure occurs, they must switch to an alternate secure channel. No authority approval is required, the data is Top Secret, and the transition must be completed immediately.
4. Once secure links are established, Artificial Intelligence/Machine Learning Specialists at the Mission Planning Cell will develop and train anomaly detection models using historical SAR datasets and AOI threat models stored in SAR data repositories. Approval is required for this step, the event priority is medium, and fallback will be to ground-based anomaly detection. This must be done within 4 hours under a Secret classification.
5. When anomaly models are ready, and anomalies are detected, All-Source Intelligence Analysts and GEOINT Analysts will interpret incoming SAR imagery at the Intelligence Exploitation Facility. They will focus on SAR anomaly events. The transition is automatic, event priority is high, and if a failure occurs, manual imagery exploitation will be performed. No authority approval is required, the information remains at the Secret level, and the maximum allowed delay is 6 hours.
6. After imagery interpretation, when preliminary reports are delivered, Watch Officers and Joint Staff J2 at the Joint Operations Center (JOC) will receive preliminary

detection briefings and decide whether to transition to the Fix phase. This critical decision requires commander approval, with Top Secret data classification, and must occur immediately to avoid mission degradation.

## Fix

1. Orient Satellite for High-Precision Targeting
When a preliminary target is detected, the Attitude Determination and Control Engineers are responsible for orienting the satellite using the Attitude Control Subsystem. This activity occurs immediately at the Spacecraft Operations Center and has a high event priority. The transition is command-triggered. If orientation fails, the system should retry orientation or fall back to ground-based validation. No authority approval is required. The data handled is classified at the Secret level, and the maximum allowed delay is 5 minutes. The action is triggered by the Attitude Determination System and depends on the accuracy of target coordinates. The risk level is moderate, and no external coordination is needed.

2. Shift to Narrow-Beam High-Resolution Collection Mode
After orientation is confirmed, Satellite Operators and System Engineers shift the satellite sensors into narrow-beam, high-resolution collection mode through the Payload Control Interface. This operation is executed immediately at the Mission Control Facility and holds high event priority. The transition is system-triggered. In case of failure, sensor recalibration should be performed. No authority approval is required. The activity involves Secret-classified data, and it must complete within 10 minutes. The action is triggered by the Payload Control Software, based on a calibration profile. The risk level is moderate, and no external coordination is necessary.

3. Fuse Multi-Sensor Data to Validate Target Coordinates
Following high-resolution data capture, Ground Segment Engineers fuse SAR, EO, and LiDAR datasets using the Multisensor Data Fusion System at the Ground Data Processing Center. This action is immediate and critical to mission success. The transition is data-driven. If the fusion fails, a re-collection request must be initiated. The information is Top Secret, and the activity must be completed within 15 minutes. The triggering system is the Geospatial Processing Engine, dependent on multisensor data integrity. The risk level is high, and external coordination is required.

4. Manage Low-Latency Relay and Fix Confirmation
Upon generation of a target fix, Data Dissemination Analysts manage the relay of verified fix reports via the Tactical Communications Router at the Intelligence Dissemination Node. This activity is immediate and critical. The transition is message-driven. If issues arise, an alternate communication path must be activated. No authority approval is necessary. The classification level is Top Secret, and the maximum allowed delay is 5 minutes. The Secure Downlink Transmitter triggers this step, relying on communication integrity. The risk is high, and external coordination is necessary.

5. Verify Target Fix with Local ISR or HUMINT Assets
Upon receiving the fix confirmation, Military End Users validate the target using field ISR platforms in a forward operational environment. This critical activity demands an urgent response. The transition is confirmation-based. If initial validation fails, revalidation with secondary sources must occur. Authority approval is required to proceed. Data is Top Secret, and execution must

occur immediately. This activity is triggered by the Tactical Data Reception Center and depends on validation reports. The risk is high, and external coordination is necessary.

## Track

1. Develop Predictive Target Movement Models
When a verified target fix is obtained, Modeling and Simulation Engineers develop predictive models of target movement using behavioral, geospatial, and environmental datasets. This activity is performed immediately at the Mission Support Analysis Center and carries a high event priority. The transition is data-driven. If the modeling fails, fallback to manual tracking assumptions is required. No authority approval is needed. The intelligence is classified at the Secret level and must be completed within 15 minutes. The triggering system is the Intelligence Analysis Workstation, dependent on historical movement data. The risk level is moderate, and no external coordination is necessary.

2. Update and Optimize Onboard Tracking Algorithms
Once the predictive model is validated, Flight Software Engineers update and optimize the spacecraft's onboard tracking algorithms through the Spacecraft Software Uplink System. This action takes place immediately at the Spacecraft Development Facility and holds a high event priority. The transition is system-triggered. If updating fails, the system should revert to the previous version of the tracking software. No authority approval is required. The activity is Top Secret and must be completed within 5 minutes. The Onboard Flight Control System triggers the step based on model performance feedback. The risk level is high, and external coordination is not needed.

3. Optimize Real-Time Data Flow Across Systems
After the tracking algorithms become active, Network Engineers optimize real-time data flow across ISR systems using the ISR Distribution Gateway. This process occurs on an ongoing basis at the Network Operations Center with medium event priority. The transition is network-triggered. If issues occur, traffic should be rerouted through alternate network paths. No authority approval is required. Data is classified as Secret and must be continuously monitored. The Data Flow Manager triggers this activity based on operational traffic loads. The risk level is moderate, and external coordination is not needed.

4. Supplement Tracking Data with Ground ISR Reconnaissance
Once data flow is stabilized, Reconnaissance Marines and UAS Operators supplement space-based tracking with live ground ISR observations collected from field assets. This real-time activity is conducted in forward operational environments and has high event priority. The transition is operationally driven. If ground ISR is unavailable, fallback to space-only ISR tracking must be used. No authority approval is required. The intelligence is classified as Top Secret and monitoring is continuous. The ISR Tasking Manager triggers this action depending on ground ISR data availability. The risk level is high, and external coordination is required.

5. Deliver Live or Near-Real-Time Tracking Overlays to C2 Systems
After fusing space-based and ground ISR data, Ground Station Operators and Military End Users deliver unified tracking overlays to command and control (C2) systems through the C2 Visualization Server. This near-real-time activity occurs at the Ground Control Center and is

considered critical. The transition is data-driven. In case of failure, the last known target location overlays must be transmitted. Authority approval is required. The data is classified Top Secret and the action must occur immediately. The Target Track Visualization Engine triggers this step, relying on fused space-ground tracking feeds. The risk level is critical, and external coordination is required.

## Target

1. Validate Multi-Source Target Intelligence
When tracking overlays are received, Imagery Scientists, SIGINT Analysts, and Targeting Officers validate multi-INT datasets—including IMINT, SIGINT, HUMINT, and MASINT—using the Intel Validation Platform. This task is performed immediately at the All-Source Fusion Center and has a high event priority. The transition is analysis-driven. If validation fails, re-validation or re-collection must be requested. Authority approval is required. The data classification level is Top Secret and the validation must be completed immediately. The Intel Aggregation Engine triggers this activity based on the availability of validated intelligence packets. The risk level is high, and external coordination is required.

2. Develop Strike Solution and Weaponeering Options
After the target validation is completed, Targeting Officers and Combat Systems Officers develop strike solutions and weaponeering options based on target coordinates, identified vulnerabilities, and collateral damage estimates (CDE reports). They use the Strike Planning Workbench at the Joint Targeting Cell, acting immediately. This step has critical event priority and is command-driven. If issues arise, strike plans must be reassessed. Authority approval is required. The activity is Top Secret and must be completed immediately. The Strike Planning Workbench triggers this based on validated targeting intelligence. The risk level is critical, and external coordination is required.

3. Develop Strike Solution and Weaponeering Options
After the target validation is completed, Targeting Officers and Combat Systems Officers develop strike solutions and weaponeering options based on target coordinates, identified vulnerabilities, and collateral damage estimates (CDE reports). They use the Strike Planning Workbench at the Joint Targeting Cell, acting immediately. This step has critical event priority and is command-driven. If issues arise, strike plans must be reassessed. Authority approval is required. The activity is Top Secret and must be completed immediately. The Strike Planning Workbench triggers this based on validated targeting intelligence. The risk level is critical, and external coordination is required.

4. Perform Final Risk, Policy, and ROE Reviews
When targeting integration is complete, Mission Assurance Analysts and representatives from the Under Secretary of Defense for Intelligence conduct final risk assessments, policy compliance reviews, and Rules of Engagement (ROE) validations. This occurs through the Policy Review Board Portal at Command Authorities immediately. The event priority is critical and policy-driven. If reviews fail, strike packages must be resubmitted for correction. Authority approval is mandatory. Data remains Top Secret and must be processed immediately. The ROE Validation Tool triggers this step based on completed risk and ROE compliance documentation. The risk level is critical, and external coordination is necessary.

5. Disseminate Strike Packages to Execution Forces

Once final ROE approval is obtained, Program Managers, Targeting Officers, and Ground Station Operators disseminate finalized strike packages to execution forces using the Secure Mission Distribution Network. Dissemination occurs immediately at the Joint Mission Planning Conference and is critical in priority. The transition is command-driven. If dissemination fails, packages must be retransmitted or manually verified. Authority approval is required. Data remains Top Secret and must be handled immediately. The Secure Transmission Gateway triggers this activity upon receiving receipt acknowledgment from execution units. The risk level is critical, and external coordination is required.

## Engage

1. Establish Real-Time Communications with Strike Assets
Once the strike package dissemination is complete, Radio Frequency and Communications Engineers and Joint Staff J6 Personnel establish real-time communications with strike assets using the C2 Communications Architecture. This occurs immediately at the Operations Communications Center with critical event priority. The transition is system-triggered. If communication fails, the fallback action is to switch to an alternate communications path. Authority approval is required. Data is classified as Top Secret and must be established immediately. The COMSEC Authentication System triggers this step, ensuring communication link authentication. The risk level is high, and external coordination is necessary.

2. Support Kinetic or Non-Kinetic Engagement Execution
After real-time communication is established, Strike Forces and Cyber Warfare Specialists support kinetic or non-kinetic engagement execution using the Strike Execution Interface onboard strike platforms. This action is taken immediately upon communication confirmation with a critical event priority. The transition is command-driven. If execution fails, fallback procedures require aborting or reverting to fallback strike plans. Authority approval is required. Data is Top Secret, and action must be immediate. The Mission Authorization Relay System triggers this based on confirmed strike orders. The risk level is critical, and external coordination is necessary.

3. Maintain ISR and Battle Tracking During Strike Window
As engagement is initiated, Ground Station Operators and ISR Operators maintain ISR coverage and battle tracking using the ISR Persistence Manager in real-time across tactical operational areas. The event priority is high and the transition is ISR-driven. In case of ISR failure, reassignment to alternate ISR platforms is required. No authority approval is needed for reassignment actions. Data classification is Secret, and monitoring must be continuous. The ISR Real-Time Relay Gateway triggers this based on ongoing ISR surveillance feeds. The risk level is moderate, and external coordination is needed.

4. Coordinate Battle Damage Assessment (BDA) Report
Following engagement completion, Ground Station Operators and BDA Analysts coordinate initial Battle Damage Assessment (BDA) reports by leveraging post-strike imagery and strike telemetry using the BDA ISR Tasking Module. This happens near-real-time at Mission Exploitation Centers. The event priority is high and the transition is event-driven. If needed, additional ISR collection is cued for further validation. Authority approval is not mandatory at this step. Data classification is Secret, and response must occur within minutes. The BDA Collection Server triggers this phase with collected BDA imagery. The risk level is moderate, and external coordination is needed.

5. Ensure Engagement Closure and Tactical Reporting
When BDA imagery analysis is initiated, Watch Officers and Operational Commanders ensure engagement closure and submit tactical reporting using the Battle Reporting Network at the Joint Operations Center. This happens near-real-time and is treated as critical. The transition is

command-driven. If the engagement outcome is unsatisfactory, commanders must issue an immediate re-engagement warning. Authority approval is mandatory. Data remains Top Secret and must be processed immediately. The Strike Monitoring Console triggers this step based on confirmed engagement outcomes. The risk level is high, and external coordination is required.

## Assess

1. Conduct Immediate Post-Strike ISR Collection
After receiving the strike completion signal, Thermal Engineers and ISR Operators conduct immediate post-strike ISR collection, focusing on SAR, EO, and thermal imagery using ISR Collection Platforms. This occurs immediately at Mission Exploitation Centers with high priority. The transition is system-triggered. If collection fails, alternate ISR collection platforms must be cued. Authority approval is not required at this step. The information is classified as Secret, and action must occur within minutes. The ISR Tasking Gateway initiates this step, depending on the availability of collected post-strike data. The risk is moderate, and external coordination is needed.

2. Analyze and Compare Pre- and Post-Strike Imagery
Once post-strike imagery is received, Imagery Scientists and All-Source Analysts analyze and compare it with pre-strike baseline imagery using the Battle Damage Assessment (BDA) Workstation at the Target Exploitation Facility. This analysis occurs near-real-time and is treated with high priority. The transition is data-driven. If discrepancies are found, analysts may request additional ISR. Authority approval is not mandatory. The data is classified as Top Secret and must be analyzed within 1 hour. The BDA Analysis Software triggers this process based on access to pre- and post-strike imagery. The risk is moderate, and external coordination is needed.

3. Assess Battle Damage and Update Target Status
After completing BDA analysis, Operational Commanders and Targeting Cells assess battle damage and update the target status using the Target Management System at Operational Command Posts. This action is critical and analysis-driven. If assessments are incomplete, they must be flagged for follow-up. Authority approval is required. The outputs are classified as Top Secret and must be processed immediately. The Functional Assessment Module triggers this step by reviewing completed BDA reports. The risk level is high, and external coordination is required.

4. Coordinate BDA Reporting and Dissemination
When the target status is updated, Watch Officers and Intel Liaisons coordinate the dissemination of finalized BDA reports through the BDA Reporting Tool at the Joint Intelligence Watch Center. This happens immediately and is high priority. The transition is report-driven. If dissemination fails, BDA reports must be resent through alternate channels. Authority approval is necessary. The data remains Top Secret and must be disseminated immediately. The Secure Intel Dissemination Network triggers this process, ensuring reports reach all required nodes. The risk is moderate, and external coordination is needed.

5. Initiate Follow-On Tasking or Reattack Planning (if required)
Based on the commander's assessment of BDA results, Mission Schedulers and Operational Planners initiate follow-on tasking or reattack planning by updating tasking requirements using the Collection Management System at Operational Planning Nodes. This phase is critical, commander-driven, and must ensure revised PIRs (Priority Intelligence Requirements) are fed into future operations. Authority approval is required. Information is classified as Top Secret and must

be updated within 1 hour. The Commander’s Operational Planning System triggers this task based on BDA gap identification. The risk is high, and external coordination is necessary.

# INTELLIGENCE CYCLE: TCPED - STATE MACHINES

## Tasking

1. Gather Priority Intelligence Requirements (PIRs)
After operational planning is completed, Defense Space Policy Analysts gather Priority Intelligence Requirements (PIRs) using the PIR Management Portal at the National Space Policy Directorate. This action is automatic and carries high priority. If the PIR gathering process encounters issues, re-validation must be requested. Authority approval is required. Information is classified as Secret and must be processed within 6 hours. The PIR Management Portal triggers this activity, with no prior data dependency. The risk is medium and no external coordination is required.

2. Rank PIRs by Mission Urgency
When new PIRs or updates are received, Defense Space Policy Analysts prioritize intelligence needs based on mission urgency using the Prioritization Engine. This occurs at the National Space Policy Directorate with high priority. The transition is automatic. If issues arise, the process should return to the gathering phase. No authority approval is required for ranking. The data is classified as Secret and must be completed within 4 hours. The Prioritization Engine triggers this step, relying on updated PIR data. The risk remains medium, with no external coordination needed.

3. Validate Tasking Requirements
Upon completion of the ranked PIR matrix, the Director of the Defense Intelligence Agency and the Deputy Assistant Secretary of Defense for Space and Intelligence validate the tasking requirements using the Tasking Validation System at the Pentagon Intelligence Coordination Office. This is a manual transition, high in priority. If validation fails, the tasking requirements must be reviewed again. Authority approval is required. Classified as Secret, the task must be completed within 6 hours. The Tasking Validation System triggers this validation, using the ranked PIR matrix as input. The risk is high, with external coordination required.

4. Deconflict Collection Plans
After validated tasking orders are generated, United States Space Command Liaison Officers deconflict collection plans using the Mission Conflict Resolver at the Combined Space Operations Center (CSpOC). This action is automatic and critical in priority. If conflicts persist, assets must be reassessed. Authority approval is required. Data is classified as Secret and must be resolved within 3 hours. The Mission Conflict Resolver triggers the process based on asset availability data. Risk is high and external coordination is necessary.

5. Finalize Collection Assignments
Once a conflict-free schedule is available, Payload Engineers and Mission Systems Architects finalize collection assignments through the Collection Assignment Module at the Space Mission Configuration Division. This is an automatic, high-priority action. If asset matching fails, retries are permitted. No authority approval is needed. It is classified as Secret and must be processed within 3 hours. The Collection Assignment Module triggers this step, based on asset deconfliction data. The risk is medium and external coordination is not required.

6. Create ISR Tasking Message Packages
Following assignment completion, Payload Engineers create ISR tasking message packages using the ISR Tasking Generator at the Space Mission Configuration Division. This is an automatic, medium-priority process. If generation fails, message packages must be validated manually. Authority approval is not required. Data is classified as Secret and should be generated within 2 hours. The ISR Tasking Generator triggers this step based on assignment outputs. The risk is low and no external coordination is necessary.

7. Apply Classification and Distribution Labels
Once ISR tasking messages are ready, Ground Station Operators apply final classification and distribution labels using the Data Classification Engine at the Mission Operations Center. This is a manual, high-priority task. If label application fails, compliance must be rechecked. Authority approval is necessary. The task is classified as Secret and must be completed within 1 hour. The Data Classification Engine triggers this operation, processing classified packages. The risk is low and external coordination is not needed.

8. Securely Transmit ISR Tasking Orders
After classification, Ground Station Operators securely transmit the ISR tasking orders using the Secure Tasking Transmission Node at the Mission Operations Center. This critical, automatic step ensures delivery of tasking orders. If transmission fails, a reattempt must occur. Authority approval is required. The information is classified as Secret and must be completed within 30 minutes. Secure Tasking Transmission Node triggers this, relying on secure communication channels. The risk is high and external coordination is not necessary.

9. Confirm ISR Asset Readiness
Finally, once secure transmission is acknowledged, Ground Station Operators confirm ISR platform readiness using the Platform Readiness Monitor at the Mission Operations Center. This is a critical, manual task. If issues are detected, alternate tasking orders must be issued. Authority approval is necessary. Data is classified as Secret and confirmation must occur within 30 minutes. The Platform Readiness Monitor triggers this step based on telemetry and health data. The risk remains high and external coordination is required.

## Collection

1. Position Platform for Optimal Collection
When tasking orders are issued, the spacecraft adjusts its orbital path to position for optimal collection using the Mission Planning Control System. This action occurs along assigned orbital paths and is high priority with an automatic transition. If positioning fails, the system will replan the orbital path. Authority approval is not required. The data classification level is Secret and the action must occur within 3 hours. The Mission Planning Control System triggers this step based on tasking confirmation data. Risk is medium and no external coordination is needed.

2. Activate Payload Sensors
Once the platform is positioned over the Area of Interest (AOI), Ground Station Operators activate the payload sensors through the Payload Activation Controller at the Satellite Control Facility. This is a high-priority automatic operation. If activation fails, the system will retry activation commands. No authority approval is necessary. Data is classified as Secret and must be completed within 1 hour. This step is triggered by the Payload Activation Controller using sensor readiness signals. The risk is medium and no external coordination is needed.

3. Collect Raw Intelligence Data
After successful sensor activation, the spacecraft begins collecting raw intelligence data using the Onboard Collection Systems while in the AOI. This action is high priority and transitions automatically. If data collection fails, the system will re-initiate the collection sequence. No authority approval is needed. It is classified as Secret and must be completed within 2 hours. This is triggered by telemetry from the Onboard Collection Systems. The risk is medium with no external coordination required.

4. Select Sensor Collection Modes
Once sensors are actively collecting, the spacecraft selects the appropriate sensor collection modes based on tasking details, using the Payload Configuration Manager. This is a medium-priority automatic transition. If selection fails, it reverts to default modes. No authority approval is needed. Data remains Secret and must be completed within 15 minutes. This is triggered by mission triggers coming into the Payload Configuration Manager. The risk is low and no external coordination is needed.

5. Dynamically Reconfigure Based on Triggers
Upon detecting significant events, the spacecraft dynamically reconfigures its sensors using the Onboard AI/ML Decision Engine. This is a high-priority automatic action. If reconfiguration fails, the system will retry event classification. No authority approval is required. Classified as Secret, this must happen immediately. The AI/ML Decision Engine triggers it using event metadata. Risk is high and no external coordination is necessary.

6. Prioritize High-Value Event Collection
If a critical event is identified, the spacecraft prioritizes high-value event collection with assistance from the Real-Time Collection Manager. This is a critical, automatic action. If prioritization fails, the data is stored as a non-priority event. No authority approval is needed. The

information remains Secret and the action must happen immediately. The Real-Time Collection Manager triggers this step using prioritized data streams. Risk is high, and no external coordination is needed.

7. Perform Integrity Checks on Collected Data
Once raw data is collected, the spacecraft performs integrity checks using the Onboard Data Validator. This is a high-priority automatic operation. If integrity checks fail, reprocessing will be attempted. No authority approval is needed. Data is classified Secret and checks must happen immediately. The Onboard Data Validator triggers the step using raw sensor files. Risk is medium and no external coordination is needed.

8. Encrypt Collected Datasets for Transmission
After integrity validation, collected datasets are encrypted using the Data Encryption Suite onboard the spacecraft. This action is high priority and automatic. If encryption fails, it will retry. No authority approval is required. Data classification remains Secret and must be completed immediately. The Data Encryption Suite triggers the encryption based on validated ISR data. Risk is medium and no external coordination is needed.

9. Queue Data for Downlink or Relay
Upon encryption completion, the spacecraft queues the data for downlink or relay using the Onboard Data Queue Manager. This is a critical automatic task. If queuing fails, the system prioritizes queued packets. No authority approval is needed. Data remains Secret and queuing must happen immediately. The Data Queue Manager triggers it with encrypted ISR packets. Risk is high and external coordination is required.

10. Task Local ISR/UAS Teams for Ground Collection
At the initiation of the ISR collection cycle, Military End Users task local ISR or UAS teams for supplemental ground collection using the Tactical ISR Tasking Portal. This is a medium-priority manual step. If support confirmation fails, a reattempt must occur. Authority approval is required. Data is classified Secret and this must happen within 3 hours. The Tactical ISR Tasking Portal triggers the action based on local ISR coordination needs. Risk is medium and external coordination is required.

11. Integrate Ground ISR Data into Collection Queue
After ground ISR collection, Ground Station Operators integrate the data into the existing collection queue using the ISR Data Fusion Node. This is a high-priority automatic task. If fusion fails, the step will retry. No authority approval is needed. Data remains Secret and must be integrated within 1 hour. The ISR Data Fusion Node triggers this operation using ground ISR data products. Risk is medium and no external coordination is needed.

12. Prioritize Combined ISR Data for Transmission
Once space and ground ISR datasets are fused, Ground Station Operators prioritize the transmission order using the Data Prioritization Manager. This is a high-priority automatic task. If prioritization fails, the system retries transmission order generation. No authority approval is needed. Data remains classified as Secret and must be completed within 30 minutes. The Data

Prioritization Manager triggers this using fused ISR packets. Risk is medium and external coordination is required.

## Processing

1. Apply Edge-Triage Algorithms
The onboard edge processor automatically applies AI-based triage algorithms to identify high-priority segments within the raw collected datasets. These algorithms enable efficient tagging of data, which results in triage-labeled outputs.

2. Generate Metadata and Confidence Scores
Once triage is complete, the metadata generator enriches the labeled data by attaching confidence scores, labels, and timestamps. This enhances the dataset's discoverability and downstream filtering, producing metadata-enhanced outputs.

3. Queue Priority Data for Immediate Downlink
The priority data manager organizes metadata-enhanced datasets into a downlink queue, prioritizing the transmission of intelligence that reflects critical mission events. This ensures time-sensitive data is relayed to ground stations first.

4. Decrypt Incoming Data Streams
After the spacecraft downlinks encrypted ISR packets, the secure decryption node on the ground automatically decrypts them using authorized encryption keys. The result is decrypted ISR data, ready for integrity checks.

5. Validate Data Integrity and Completeness
The data integrity validation system reviews decrypted ISR packets to ensure all data is complete and error-free. Validated ISR files are then passed on for categorization and analysis.

6. Categorize Data by Intelligence Domain
Using the data categorization engine, validated ISR files are sorted into domain-specific repositories—such as IMINT, SIGINT, MASINT, HUMINT, or multi-INT folders—allowing specialized teams to exploit them efficiently.

7. Deploy Pre-Trained ML Models
AI pipelines are triggered by the intelligence pre-processing node, which applies object recognition, RF pattern analysis, and other detection models to categorized ISR data. The outputs are ML-labeled intelligence products.

8. Prioritize High-Confidence Results
The confidence sorting engine ranks the machine-labeled outputs based on model confidence scores. This step surfaces high-confidence intelligence for faster exploitation, creating a prioritized product list.

9. Flag Anomalies for Immediate Review
The anomaly detection algorithm scans processed ISR streams to flag irregularities or urgent events requiring human analyst review. This results in anomaly alerts and datasets for high-priority human exploitation.

10. Apply Classification and Handling Markings

The intelligence classification manager assigns appropriate security labels and handling instructions to processed intelligence. This ensures data complies with distribution control and results in properly classified files.

11. Package Data for Exploitation Systems
Using the exploitation packaging engine, classified intelligence is formatted into standard structures compatible with GEOINT, SIGINT, or analyst systems. These ready-to-use packages support rapid exploitation.

12. Distribute to Exploitation Centers
Finally, the secure intelligence data bus transmits exploitation packages to analyst nodes or fusion centers. The data becomes immediately available at analyst workstations, enabling the next step in the TCPED pipeline.

## Exploitation

1. Load Processed Intelligence Packages
When processed data becomes available, ground station operators load these packages into analyst workstations using dedicated interfaces. This action is automatically triggered and prepares the system for screening. If issues occur, the system retries the dataset load.

2. Perform Preliminary Screening
Once datasets are loaded, intelligence analysts automatically begin preliminary screening using specialized software. This identifies anomalies or points of interest. If errors are encountered, the screening process is retried without human intervention.

3. Flag Critical Intelligence Items
If high-value targets or significant findings are detected during screening, analysts flag them using a triage dashboard. These flagged items become priority alerts for follow-on exploitation. Reflagging is supported if anomalies are re-evaluated.

4. Conduct Specialized Domain Analysis
Upon flagging priority targets, domain experts (e.g., GEOINT, SIGINT, MASINT analysts) perform deep analysis using exploitation toolkits. This yields domain-specific reports, and failures trigger reassignment to other domain analysts.

5. Cross-Correlate Multi-INT Sources
Once domain reports are available, multi-INT analysts use a fusion engine to correlate and synthesize data across all intelligence domains. If fusion fails, the system retries the process using backup correlation logic.

6. Derive Operationally Relevant Insights
Fused multi-source data is interpreted by analysts to extract mission-relevant insights. These results are passed to planners, and clarification may be requested if inconsistencies arise during synthesis.

7. Validate Intelligence Findings and Assess Confidence
Once insights are drafted, senior analysts use a confidence assessment module to validate and rate each finding. This step ensures that each intelligence product reflects both data quality and analytical rigor.

8. Assign Confidence Ratings
Following validation, analysts assign formal confidence ratings to intelligence outputs. These metrics guide consumers on reliability and risk. Errors in scoring trigger revalidation cycles automatically.

9. Generate Source Validation Audit Trail
Analysts then generate source validation audit trails, documenting how conclusions were derived and which sources were used. This ensures traceability and supports forensic auditing.

10. Produce Visual Overlays and Geospatial Products

Once audit records are finalized, analysts use geospatial tools to produce visual intelligence products, including overlays, maps, and annotations that visually express key intelligence findings.

11. Draft Intelligence Reports and Bulletins
Analysts use authoring portals to compile visual products and insights into written reports and mission bulletins. These are formatted for operational briefings and command review.

12. Package Final Intelligence Products
Once the reports are finalized, they are packaged by the intelligence packaging manager. These packages are prepared for secure transmission to end users and dissemination hubs.

## Dissemination

1. Consolidate Exploited Intelligence Products
When final intelligence products become available, ground station operators use the Intelligence Product Compiler to consolidate reports, visuals, and data into cohesive packages. This step is automatically triggered and retries compilation if needed.

2. Apply Final Classification and Distribution Labels
Once products are consolidated, classification officers apply final security markings and distribution labels using the Classification Management Tool. This action is automated, ensuring products meet classification protocols before dissemination.

3. Approve Packages for Release
Upon classification, release authorities manually review packages for accuracy and compliance using the Release Authority Review Portal. Approval is mandatory, and the process includes fallback mechanisms if issues arise during the review.

4. Determine Recipient Lists Based on Operational Roles
After release approval, distribution officers use the Dissemination Routing System to match recipients based on operational relevance. The system automatically assigns dissemination routes, with retry options for recipient mapping errors.

5. Securely Transmit Products to C2 and IC Systems
With recipient lists confirmed, ground station operators transmit the products via secure networks using the Secure Transmission Gateway. This process is automatic and supports retries if transmission issues occur.

6. Confirm Receipt and Access Acknowledgements
Once products are delivered, operators validate receipt using the Receipt Validation Module to confirm that all intended users have accessed the materials. This step ensures accountability and completeness of dissemination.

7. Identify Critical Intelligence for Immediate Action
If any disseminated products contain urgent information, watch officers use the Critical Intelligence Filter to identify items that warrant real-time alerts. This step is critical and automatically triggers if alert criteria are met.

8. Issue Real-Time Intelligence Alerts
When critical items are confirmed, watch officers use the Tactical Alerting Network to broadcast flash alerts to relevant commanders and tactical elements. The system is designed for high-priority, immediate dissemination.

9. Log Alert Dissemination for Audit and Traceability
Following alert issuance, dissemination logs are created via the Alert Dissemination Log System to track who received which alert and when. These logs support post-mission audits and traceability.

10. Collect User Feedback on Intelligence Utility

Intelligence officers collect feedback from end users through the Intelligence Feedback Portal. This feedback helps assess the relevance and clarity of disseminated products and is stored for refinement analysis.

11. Analyze Feedback for Refinement Opportunities
Feedback is then processed by intelligence officers using the Feedback Analysis Engine. This analysis identifies any gaps or inefficiencies in the intelligence products or delivery mechanisms.

12. Update Collection/Tasking Based on Feedback
Finally, intelligence managers use the Collection Retasking System to update tasking priorities based on refined insights and user needs. This step concludes the cycle and prepares for the next iteration of TCPED.