HUMINT CONTROL SYSTEM (HCS) DOCUMENT
ACCESS RESTRICTED TO BIGOT LIST ALPHA — SEE SECTION B-1.2 FOR ACCESS REQUIREMENTS

NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE
CYBERSECURITY THREAT INTELLIGENCE DIRECTORATE
HUMINT Operations Cell | Fort George G. Meade, Maryland 20755

ANNEX B TO NSA-CTI-2024-0391-B

[REDACTED] HIGH SCHOOL INCIDENT
COMMUNITY NEXUS DETAILED ASSESSMENT

Soyjak.party Platform — Pre-Incident Activity, Actor Attribution, and Radicalization Pathway Analysis

PARENT DOCUMENT:	NSA-CTI-2024-0391-B (Soyjak.party Platform Threat Assessment)
ANNEX SERIAL:	NSA-CTI-2024-0391-B/B
DATE:	04 MARCH 2024
CLASSIFICATION:	TOP SECRET // SI // HCS // NOFORN
ACCESS CONTROL:	BIGOT LIST ALPHA (see B-1.2)
ORIGINATOR:	NSA/CTID — HUMINT Operations Cell + FBI BAU (Joint)
DISSEMINATION:	BIGOT LIST ALPHA ONLY — NOT FOR WIDER IC RELEASE

HCS HANDLING AND CONTROL NOTICES:

This document contains information derived from and/or identifying clandestine human intelligence (HUMINT) sources. Unauthorized disclosure of HCS information is a federal crime under 50 U.S.C. § 3121 (Intelligence Identities Protection). This document may NOT be reproduced, summarized, paraphrased, or transmitted by any means without prior written authorization from the NSA/CSS HUMINT Operations Cell Supervisor. Do not discuss contents in non-secure facilities. If this document is found outside authorized channels, contact NSA Security Operations Center: (301) 688-XXXX.

■ BIGOT LIST ALPHA NOTE:

Bigot List Alpha is maintained by the NSA/CTID Security Officer. Individuals not on Bigot List Alpha who receive this document in error must immediately report to their security officer and return or destroy all copies. Reading further constitutes acknowledgment of authorization and acceptance of handling responsibilities.

B-1. PURPOSE, SCOPE, AND ACCESS REQUIREMENTS

B-1.1 Purpose

(U//FOUO) This annex provides the complete joint NSA/FBI assessment of the relationship between Soyjak.party community activity and the [REDACTED] High School incident of [REDACTED] 2025. It documents the full body of SIGINT and HUMINT collection bearing on the incident, the analytical process by which a potential nexus was identified and evaluated, the results of coordinated investigative activity with the Federal Bureau of Investigation, and the analytical conclusions and confidence assessments reached by the joint assessment team.

(U//FOUO) This annex is a companion to and should be read in conjunction with the parent document (NSA-CTI-2024-0391-B) and with FBI Case File [REDACTED], copies of which are maintained by the NSA/CTID HUMINT Operations Cell and are available to Bigot List Alpha personnel upon request through secure channels.

B-1.2 Access Requirements and Bigot List Alpha

(TS//HCS//NF) This annex is classified TOP SECRET // SPECIAL INTELLIGENCE // HUMINT CONTROL SYSTEM // NOFORN. Access is restricted to Bigot List Alpha, which is maintained by the NSA/CTID Security Officer. Bigot List Alpha was established specifically for this collection program in September 2021 and currently includes [REDACTED] cleared personnel across NSA/CSS, FBI, and [REDACTED] other agencies. The list is reviewed and recertified on a 90-day basis.

(TS//HCS//NF) The HCS control designation is applied because this annex contains information that, if disclosed, could reasonably be expected to: (a) identify or allow the identification of one or more clandestine human sources; (b) compromise ongoing collection operations; or (c) prejudice active federal criminal proceedings. These three concerns are of varying weight across different sections of this annex, as noted in the relevant section headers.

B-1.3 Coordination History

DATE	PARTIES	ACTION / MILESTONE
Oct 2021	NSA/CTID	Initial HUMINT tasking for platform; Bigot List Alpha es
Sep 2022	NSA/CTID + FBI CyD	Initial interagency coordination meeting; MOU executed
[REDACTED] 2	NSA/CTID + FBI CyD + B	Incident occurs; joint nexus investigation initiated wit
[REDACTED] 2	NSA/CTID + FBI BAU	NSA provides SIGINT technical support package to FBI
[REDACTED] 2	Joint Team	Preliminary nexus assessment issued (now superseded by t
Mar 2024	Joint Team	This final assessment finalized and approved for dissemi

(S//NF) NSA's role in the joint investigation has been limited to signals intelligence support and does not extend to law enforcement functions. All law enforcement activity, including evidence collection, interviews, and prosecutorial referrals, has been conducted exclusively by the FBI under applicable Title 18 authorities. NSA collection products provided to the FBI were reviewed by NSA/OGC to ensure compliance with applicable legal standards prior to dissemination.

B-2. INCIDENT SUMMARY (U//FOUO)

(U//FOUO) The following summary of the incident is derived entirely from open-source reporting and law enforcement information provided to NSA/CTID by the FBI under the interagency MOU. No NSA collection assets were tasked against the incident itself or against any of its participants in an anticipatory capacity. This summary is included for analytical context only. Operational details of the FBI criminal investigation are contained in FBI Case File [REDACTED] and are not reproduced in this annex.

INCIDENT OVERVIEW — OPEN SOURCE / LAW ENFORCEMENT DERIVED (U//FOUO)

INCIDENT DATE:	[REDACTED] 2025
LOCATION:	[REDACTED] High School, [REDACTED], United States
INCIDENT TYPE:	Targeted mass casualty event, educational facility
CASUALTIES:	[REDACTED] (law enforcement figures — not reproduced here)
SUBJECT(S):	[REDACTED] — identity withheld per 50 U.S.C. § 3121 / ongoing proceedings
PRIMARY LE AGENCY:	FBI Field Office [REDACTED] / local law enforcement in support

(U//FOUO) The incident came to the attention of NSA/CTID through two independent channels: first, through automated monitoring of platform activity, which detected an anomalous spike in discussion volume and content patterns consistent with a significant external event of interest to the community; and second, through direct notification from FBI Field Office [REDACTED], which contacted NSA/CTID's interagency liaison within [REDACTED] hours of the incident based on preliminary investigative leads suggesting possible online community connections.

(S//NF) The preliminary investigative lead that prompted FBI notification to NSA was derived from digital device examination of material seized pursuant to a search warrant. Specific details of that examination are contained in FBI Case File [REDACTED] and are not reproduced here. NSA was notified for the purpose of providing technical SIGINT support and historical collection data relevant to platform-associated actors. The FBI's notification was consistent with the terms of the interagency MOU established in September 2022.

B-3. INITIAL NEXUS IDENTIFICATION AND ASSESSMENT TRIGGER

(TS//SI//NF) Prior to receiving the FBI notification, NSA UPSTREAM collection and XKS monitoring had already flagged anomalous platform activity beginning approximately [REDACTED] hours after the incident. Automated keyword and pattern-of-life alerts generated by the CTID/SIGDIV watch floor identified an approximately [REDACTED]% increase in posting volume on the platform's primary board, combined with content patterns — specifically, the sustained discussion of a specific geographic location and an event matching the incident's profile — that exceeded the threshold for watch floor escalation.

(TS//SI//NF) Watch floor escalation triggered a manual review by a CTID/OSIB senior analyst, who confirmed that platform content appeared to contain: (a) discussion of the incident using accurate details not yet publicly reported, raising the possibility of foreknowledge or participant presence; (b) expressions of approval by a subset of users; and (c) references to one or more usernames that had appeared in prior NSA collection as potentially significant. The senior analyst elevated the finding to the CTID Division Chief, who authorized immediate escalation to the HUMINT Operations Cell and FBI interagency liaison.

(TS//SI//HCS//NF) ASSET YELLOWJACKET, the CTID's primary embedded HUMINT source, was contacted by handler [REDACTED] within [REDACTED] hours of the incident. ASSET YELLOWJACKET provided an initial oral report indicating awareness of relevant platform activity and identifying [REDACTED] specific usernames that had attracted community attention in connection with the incident. YELLOWJACKET's initial report is summarized in Section B-5 of this annex.

B-4. PRE-INCIDENT SIGINT COLLECTION FINDINGS

(TS//SI//NF) Following FBI notification and CTID watch floor escalation, CTID/SIGDIV analysts conducted a retrospective review of all NSA holdings bearing on platform-associated activity that might be relevant to the incident. This review covered a [REDACTED]-month lookback period and drew on UPSTREAM collection, XKS stored data, DNS metadata holdings, and cross-platform correlation products. The following findings represent the totality of pre-incident SIGINT material assessed as potentially relevant to the community nexus question.

B-4.1 Pre-Incident Platform Posting Activity — Relevant Excerpts

(TS//SI//NF) Retrospective review of XKS stored content identified [REDACTED] posts on the platform in the [REDACTED]-month period preceding the incident that contain content assessed as potentially relevant to the nexus question. These posts fall into three categories: (a) posts containing expressions of generalized violent ideation directed at educational institutions, which are common on the platform and assessed as predominantly performative rather than operational; (b) posts that appear to reference a specific geographic area consistent with the incident location, which are fewer in number and assessed as warranting closer examination; and (c) posts attributed with varying confidence levels to usernames of interest identified through the HUMINT reporting described in Section B-5.

(TS//SI//NF) Category (a) posts are assessed as LIKELY NOT DIRECTLY RELEVANT to the incident. Violent ideation content of the type described is endemic to the platform and to comparable anonymous imageboard communities and does not, in the analytic judgment of CTID/OSIB, represent a meaningful behavioral precursor in this context absent corroborating specificity. FBI BAU concurs with this assessment.

(TS//SI//NF) Category (b) posts — those referencing a specific geographic area consistent with the incident location — number [REDACTED] in total. Of these, [REDACTED] were made by IP addresses or behavioral fingerprints attributable with MODERATE or HIGH CONFIDENCE to actors of interest identified in ANNEX D. Content of these posts is summarized in the table below. Verbatim content is maintained in the CTID analytical holdings and is available to Bigot List Alpha personnel through the NSANet portal.

POST ID	TIMING	RELEVANCE	CONTENT SUMMARY	ATTRIBUTION
[RED]-01	[RED] months	LOW	Geographic reference, non-specific. Ro	Unattributed
[RED]-02	[RED] months	LOW	Geographic reference with school conte	Unattributed
[RED]-03	[RED] weeks p	MODERATE	Geographic + institutional reference.	USERNAME-A (MOD CONF
[RED]-04	[RED] weeks p	MODERATE	Cross-references [RED]-03. Different I	USERNAME-A (MOD CONF
[RED]-05	[RED] days pr	HIGH	Geographic, institutional, and tempora	USERNAME-A (HIGH CON
[RED]-06	[RED] days pr	HIGH	Response to [RED]-05 by separate user.	USERNAME-B (LOW CONF

(TS//SI//NF) POST [RED]-05 is assessed as the most analytically significant pre-incident item. Its content, which is reproduced in full in the classified appendix to this annex (available to Bigot List Alpha via NSANet), contains a level of specificity that CTID analysts assessed — after consultation with FBI BAU — as inconsistent with the generalized violent ideation common to the platform. The post was not flagged by automated systems prior to the incident; it fell below automated threshold parameters because it did not contain the specific keywords programmed into XKS alert rules. This represents a collection gap of the type described in ANNEX A, Section A-5.

B-4.2 Pre-Incident Cross-Platform Activity

(TS//SI//NF) Cross-platform correlation analysis (see ANNEX A, Section A-3.7) identified [REDACTED] accounts on external platforms assessed with varying confidence as operated by the same individual(s) attributed to Posts [RED]-03 through [RED]-05. Activity on these external platform accounts during the pre-incident period is summarized below. Full correlation methodology and confidence scoring is documented in CTID product CTID-XPC-2022-003.

(TS//SI//NF) External platform activity during the relevant period included [REDACTED] increased engagement with content

B-4.3 Private Communications — SIGINT-Derived (TS//SI//NF)

■ HCS ACCESS RESTRICTION:
The following section contains HUMINT Control System (HCS) information identifying or derived from clandestine human sources. Access is restricted to BIGOT LIST ALPHA. Contact NSA/CSS Security Officer before further dissemination.

(TS//SI//HCS//NF) NSA SIGINT collection captured [REDACTED] private communications during the pre-incident period that are assessed as relevant to the nexus question. These communications occurred on platforms with varying levels of NSA collection coverage and involve accounts attributed with varying confidence to subjects of interest. Verbatim content is maintained in CTID analytical holdings and has been provided to FBI under the interagency MOU. Summaries only are reproduced here.

(TS//SI//HCS//NF) COMMUNICATION SET ALPHA: [REDACTED] messages between accounts attributed to USERNAME-A and an unidentified second party, occurring approximately [REDACTED] weeks before the incident. Content includes: references to the geographic area of interest; discussion of a planning timeline; and [REDACTED]. These communications were collected under [REDACTED] authority and reviewed by NSA/OGC for U.S. person handling prior to provision to FBI. They represent the highest-confidence pre-incident SIGINT item.

(TS//SI//HCS//NF) COMMUNICATION SET BETA: [REDACTED] messages on a separate platform attributed with LOW CONFIDENCE to USERNAME-A. Content is ambiguous and does not, in CTID/OSIB's assessment, independently support or contradict the nexus conclusion. FBI BAU assesses these communications as potentially consistent with but not probative of the nexus. These communications are included for completeness.

(S//NF) Analysts note that the availability of private communications from this period is a function of the specific platforms used and their intersection with NSA collection coverage. There may be additional private communications on platforms without collection coverage that would alter the analytic picture. This represents a material collection gap acknowledged in the analytical conclusions in Section B-9.

B-4.4 Device and Network Forensic Correlation

(TS//SI//NF) NSA/CTID provided FBI with a technical support package consisting of: (a) all IP addresses associated with USERNAME-A's platform activity over the preceding [REDACTED] months; (b) timing and session data for those IP addresses; and (c) cross-platform identity correlation data associating USERNAME-A with accounts on [REDACTED] external platforms. This package was used by FBI to support its application for search warrants and subpoenas in the criminal investigation. The legal basis for NSA's provision of this data to FBI is documented in the interagency MOU and was reviewed by NSA/OGC prior to transfer.

(S//NF) FBI has confirmed, through independently obtained evidence, that [REDACTED] of the IP addresses provided by NSA are associated with the subject of the criminal investigation. This independent corroboration elevates the confidence of NSA's prior USERNAME-A attribution from MODERATE to HIGH CONFIDENCE for the purposes of this assessment. Additional technical forensic details are contained in FBI Case File [REDACTED] and are not reproduced here.

B-5. HUMINT COLLECTION FINDINGS

■ HCS ACCESS RESTRICTION:
The following section contains HUMINT Control System (HCS) information identifying or derived from clandestine human sources. Access is restricted to BIGOT LIST ALPHA. Contact NSA/CSS Security Officer before further dissemination.

(TS//SI//HCS//NF) HUMINT reporting from active assets contributed materially to the nexus assessment. The following summaries reflect reporting received from ASSET YELLOWJACKET and ASSET MOONRAT in the post-incident

B-5.1 ASSET YELLOWJACKET Reporting

B-5.2 ASSET MOONRAT Reporting

■ HCS ACCESS RESTRICTION:
The following section contains HUMINT Control System (HCS) information identifying or derived from clandestine human sources. Access is restricted to BIGOT LIST ALPHA. Contact NSA/CSS Security Officer before further dissemination.

(TS//SI//HCS//NF) ASSET MOONRAT, embedded within the platform's wiki-editing community, provided two reports relevant to the incident. MOONRAT's primary value in this context is visibility into the community's self-documentation and archival activity, which reflects a deliberate collective memory-management function that is analytically significant.

(TS//SI//HCS//NF) MOONRAT Report MR-07 documents that wiki editors made [REDACTED] attempts to create or expand entries related to the incident and its community nexus in the days following the event. Of these, [REDACTED] were deleted by wiki administrators within hours of creation. MOONRAT assessed this as reflecting an administrative decision to minimize the platform's documented association with the incident. MOONRAT also reported that [REDACTED] off-wiki discussions among senior editors explicitly referenced concern about law enforcement attention.

(TS//SI//HCS//NF) MOONRAT Report MR-09, received approximately [REDACTED] weeks post-incident, documents that a community archivist had privately preserved post content related to USERNAME-A and the pre-incident period before administrative deletion. MOONRAT indicated willingness to attempt to obtain this archive. Handler [REDACTED] authorized a passive acquisition attempt; outcome is pending as of the date of this annex. Any material obtained will be documented in a supplemental report.

B-6. COMMUNITY REACTION ANALYSIS

(TS//SI//NF) The community's reaction to the incident and to its potential association with the platform is itself a significant body of analytical evidence. CTID/OSIB conducted a structured analysis of platform posting behavior in the [REDACTED]-day period following the incident, drawing on UPSTREAM collection, XKS stored data, and HUMINT reporting. Key findings are described below.

B-6.1 Posting Volume and Pattern Analysis

(TS//SI//NF) Platform posting volume spiked to approximately [REDACTED]% above baseline in the [REDACTED]-hour period immediately following the incident, consistent with the pattern observed following other major external events that attract community attention. Volume returned to near-baseline within [REDACTED] days. This volume pattern does not, in isolation, distinguish between genuine community nexus and ordinary community interest in a newsworthy event; both would be expected to produce similar volume signatures.

B-6.2 Content Composition Analysis

(TS//SI//NF) Content analysis of post-incident platform content identified four distinct posting cohorts, characterized by CTID/OSIB analysts as follows:

COHORT	EST. SIZE	BEHAVIOR DESCRIPTION	ANALYTICAL NOTE
COHORT A	Approx. [RED	Expressed explicit approval or cel	HIGH concern. Small but meaningfu
COHORT B	Approx. [RED	Discussion and speculation without	LOW concern. Consistent with norm
COHORT C	Approx. [RED	Expressed discomfort, distancing,	LOW concern. Suggests awareness o
COHORT D	Approx. [RED	Active post deletion, counter-narr	MODERATE concern. May reflect coo

(TS//SI//NF) COHORT D behavior — coordinated post deletion and counter-narrative activity — is assessed as analytically significant. While post deletion is normal platform behavior for individual users, the temporal clustering and apparent coordination of deletion activity in this case exceeds what would be expected from independent individual

(TS//SI//NF) CTID/OSIB notes that the majority of the platform community — represented by COHORTS B and C

B-7. ACTOR IDENTIFICATION AND ASSESSMENT (TS//SI//HCS//NOFORN)

■ HCS ACCESS RESTRICTION:
The following section contains HUMINT Control System (HCS) information identifying or derived from clandestine human sources. Access is restricted to BIGOT LIST ALPHA. Contact NSA/CSS Security Officer before further dissemination.

(TS//SI//HCS//NF) This section summarizes the identity assessments for actors of interest identified through the nexus investigation. Full biographical dossiers are maintained in ANNEX D (TS//SI//HCS//NOFORN — Bigot List Alpha). Information in this section is intentionally limited to what is necessary to support the analytical conclusions in Section B-9. All identity information must be handled in accordance with HCS protocols and U.S. person minimization procedures.

B-7.1 USERNAME-A (Primary Actor of Interest)

(TS//SI//HCS//NF) USERNAME-A is the primary actor of interest identified through the nexus investigation. Real-world identity has been confirmed with HIGH CONFIDENCE through the combination of: NSA SIGINT IP attribution corroborated by FBI independently-obtained evidence; stylometric model attribution (CTID-ML-2023-091, HIGH CONFIDENCE output); cross-platform identity correlation linking USERNAME-A to [REDACTED] other accounts; and ASSET YELLOWJACKET reporting consistent with the SIGINT-derived attribution. Identity details are withheld from this annex and maintained exclusively in ANNEX D per HCS protocols.

(TS//SI//HCS//NF) USERNAME-A's platform activity history spans approximately [REDACTED] months of recorded NSA collection. Activity patterns show [REDACTED] total posts attributed with HIGH or MODERATE CONFIDENCE, concentrated in the platform's primary boards. Content analysis of this posting history, conducted by CTID/OSIB in coordination with FBI BAU, identified [REDACTED] posts containing ideation content assessed as potentially relevant to radicalization pathway analysis (see Section B-8). The volume of this content is not atypical for high-volume platform users; its character is assessed as at the higher end of the severity distribution for platform users in NSA's holdings.

(TS//SI//HCS//NF) NSA's jurisdiction over USERNAME-A's information is limited. The individual is assessed as a U.S. person, and all NSA-derived information has been handled under applicable minimization procedures. NSA's role is limited to SIGINT technical support; all law enforcement action is the exclusive province of FBI. NSA has not conducted and will not conduct independent investigative activity with respect to this individual beyond the SIGINT support described in this annex.

B-7.2 USERNAME-B and Secondary Actors

(TS//SI//HCS//NF) USERNAME-B was identified as a secondary actor through post-incident content analysis, specifically through its connection to Post [RED]-06 (see Section B-4.1). Real-world identity attribution for USERNAME-B is assessed at LOW CONFIDENCE and has not been corroborated through independent means. FBI has been notified of USERNAME-B as a potential subject of interest; investigative disposition is the FBI's determination to make.

(TS//SI//HCS//NF) [REDACTED] additional usernames were identified through ASSET YELLOWJACKET reporting as community members who engaged in discussion of USERNAME-A's identity in the post-incident period. These usernames are documented in ANNEX D as secondary subjects; none are currently assessed as actors of independent investigative significance. Their significance is limited to their potential evidentiary value regarding community awareness of the USERNAME-A nexus.

B-7.3 Platform Administrative Actors

(TS//SI//HCS//NF) Platform administrators (see ACTOR-2/COBBLESTONE profile, ANNEX D) are not assessed as

B-8. RADICALIZATION PATHWAY ASSESSMENT (TS//SI//NOFORN)

(U//FOUO) This section represents the joint CTID/OSIB and FBI BAU assessment of whether Soyjak.party and its content environment played a material role in any radicalization pathway associated with the incident. This assessment is presented separately from the nexus question because the two are analytically distinct: the nexus question concerns whether community-connected actors participated in the incident; the radicalization pathway question concerns whether the platform's content environment contributed to the development of the behavioral disposition that led to the incident.

(S//NF) FBI BAU's radicalization pathway analysis, conducted on the basis of its independent investigation and the NSA SIGINT support package, assessed that USERNAME-A had a documented multi-year history of engagement with online communities associated with violent ideation content. Soyjak.party was one of multiple platforms in USERNAME-A's documented online activity history. FBI BAU's full radicalization pathway assessment is contained in FBI Case File [REDACTED] and is not reproduced here; the following represents a summary provided to NSA/CTID for inclusion in this annex.

B-8.1 Platform's Role in Content Exposure

(S//NF) FBI BAU assessed that Soyjak.party was a CONTRIBUTING rather than PRIMARY factor in USERNAME-A's content exposure history. The platform's content environment — which, as documented in the parent assessment, intersects with violent ideation, accelerationist aesthetics, and far-right adjacent content — provided one node in a broader network of online radicalization exposure. FBI BAU identified [REDACTED] other platforms as higher-priority nodes in the radicalization pathway.

(S//NF) CTID/OSIB concurs with the CONTRIBUTING characterization. The platform's documented content environment is assessed as capable of normalizing violent ideation within the specific ironic-detachment context of chan-culture, which may reduce psychological barriers to violent ideation among susceptible individuals. However, the causal pathway from platform exposure to violent action is not direct and involves numerous intervening factors that are outside the scope of NSA's analytical mandate and are more appropriately assessed by FBI BAU.

B-8.2 Platform-Specific Radicalization Mechanism Assessment

(S//NF) CTID/OSIB assesses that the platform's specific radicalization mechanism, to the extent one exists, operates primarily through normalization of violent content within a framework of ironic detachment that makes psychological defenses against such content less effective. The platform's culture of performative transgression — in which expressions of violent ideation are routinely framed as humor rather than genuine advocacy — may attenuate users' awareness of their own desensitization. This mechanism is not unique to Soyjak.party and is documented across comparable anonymous imageboard communities.

(S//NF) CTID/OSIB does not assess that the platform actively recruits for or promotes violent action. The community does not exhibit the characteristics of a structured extremist organization and there is no evidence of deliberate radicalization pipeline operation. The platform's contribution to radicalization risk is best characterized as ambient and passive rather than active.

B-8.3 Applicability to Broader Platform User Base

(U//FOUO) CTID/OSIB and FBI BAU jointly caution against generalizing from this individual case to conclusions about the platform's user base as a whole. The vast majority of platform users have no connection to violent action and the available evidence does not support a characterization of the community as a radicalization pipeline in any systematic sense. The presence of one — or even several — community-connected actors in violent incidents does not, in isolation, establish a systemic causal relationship. This caveat is recorded here for the benefit of downstream analysts

(U//FOUO) Any public-facing characterization of the platform as directly associated with this or other violent incidents

B-9. FBI COORDINATION AND JOINT INVESTIGATIVE ACTIVITY

(U//FOUO) NSA's engagement with the FBI on this matter has been governed by the interagency MOU executed in September 2022 and by applicable legal authorities reviewed by NSA/OGC. This section documents the nature and scope of the coordination and describes the division of responsibilities between NSA and FBI.

B-9.1 NSA Technical Support to FBI

(S//NF) NSA provided the following technical support products to FBI under the interagency MOU. All products were reviewed by NSA/OGC prior to transfer. Products containing U.S. person information were transferred pursuant to documented FBI need and with appropriate minimization caveats.

ITEM	DESCRIPTION	CLASS.	STATUS	LEGAL REVIEW
TECH-01	IP address history for platform selec	S//NF	Provided	NSA/OGC cleared
TECH-02	Session timing and metadata	TS//SI//NF	Provided	NSA/OGC cleared
TECH-03	Cross-platform correlation summary (U	TS//SI//NF	Provided	NSA/OGC cleared
TECH-04	Stylometric attribution report (USERN	TS//SI//NF	Provided	NSA/OGC cleared
TECH-05	Pre-incident post content package (Po	TS//SI//NF	Provided	NSA/OGC cleared
TECH-06	SIGINT-derived private communication	TS//HCS//NF	Provided (sa	HCS protocols applied
TECH-07	HUMINT reporting summaries (sanitized	S//NF	Provided	Source identity withh

(S//NF) NSA has not and will not provide raw SIGINT collection to FBI for use as direct evidence in criminal proceedings. All products transferred to FBI represent processed analytical summaries. If FBI seeks to use NSA-derived information in criminal proceedings, it must do so through appropriate legal channels including, if necessary, ex parte FISA proceedings. NSA/OGC has been briefed on this requirement and is available to support FBI legal counsel on any such proceeding.

B-9.2 FBI Investigative Findings Relevant to Nexus Assessment

(S//NF) The FBI has shared the following findings from its independent investigation with NSA/CTID for incorporation into this joint assessment. These findings are drawn from FBI investigative activity and are not NSA-derived; they are included here with FBI's authorization and are attributed to FBI in all analytical products.

(S//NF) FBI FINDING 1: Device examination of material seized pursuant to search warrant confirmed the presence of platform-associated content and USERNAME-A account credentials on the subject's devices. This finding independently corroborates NSA's SIGINT-derived USERNAME-A attribution.

(S//NF) FBI FINDING 2: FBI BAU's behavioral case analysis, conducted on the basis of the full investigative record, assessed a MODERATE-HIGH probability of platform content exposure as a contributing environmental factor in the subject's behavioral history. FBI BAU cautions that contributing environmental factor is a specific term of art in behavioral case analysis and does not imply legal causation.

(S//NF) FBI FINDING 3: FBI has not identified evidence of coordination between the subject and any other platform community member in planning or executing the incident. The investigation has proceeded on the working assumption of a lone actor, consistent with behavioral case analysis findings. This working assumption remains subject to revision if new evidence emerges.

B-10. ANALYTICAL CONCLUSIONS AND CONFIDENCE ASSESSMENTS

(U//FOUO) The following analytical conclusions represent the joint assessment of NSA/CTID and FBI BAU, developed through the process described in this annex. Confidence levels follow ICD 203 standards. Where NSA and FBI assessments diverge, this is noted. Analytical disagreements within the joint team were resolved through structured analytic techniques including analysis of competing hypotheses (ACH); documentation of this process is available in CTID analytical holdings.

CONCLUSION 1 — COMMUNITY NEXUS — CONFIRMED — HIGH CONFIDENCE

(TS//SI//NF) The subject of the FBI criminal investigation was a participant in the Soyjak.party community under the username USERNAME-A. This conclusion is supported by: (a) NSA SIGINT IP attribution corroborated by FBI independently-obtained evidence; (b) HIGH-CONFIDENCE stylometric model output; (c) cross-platform identity correlation; and (d) ASSET YELLOWJACKET reporting. There is no significant competing hypothesis that adequately accounts for the totality of the evidence.

CONCLUSION 2 — FOREKNOWLEDGE BY COMMUNITY — NOT CONFIRMED — LOW CONFIDENCE ONLY

(TS//SI//NF) The evidence does not support a conclusion that community members other than the subject had foreknowledge of the incident. Post [RED]-05 and Communication Set Alpha are the primary items bearing on this question; neither independently or collectively establishes foreknowledge by a third party. The post-incident coordination behavior of COHORT D is assessed as more consistent with reputational risk management than foreknowledge.

CONCLUSION 3 — PLATFORM AS RADICALIZATION FACTOR — ASSESSED CONTRIBUTING — MODERATE CONFIDENCE

(TS//SI//NF) Soyjak.party is assessed as a CONTRIBUTING factor in the subject's content exposure history, consistent with FBI BAU's independent assessment. It is not assessed as the PRIMARY factor. This conclusion is held at MODERATE CONFIDENCE owing to the inherent limitations of retrospective radicalization pathway analysis and the absence of direct evidence of platform-specific causal influence.

CONCLUSION 4 — ORGANIZED COMMUNITY INVOLVEMENT — NOT SUPPORTED — HIGH CONFIDENCE

(TS//SI//NF) The evidence does not support a conclusion that the Soyjak.party community as an organization or any organized subset thereof was involved in planning or facilitating the incident. The incident is assessed as the act of an individual who happened to be a community member, not an act organized or facilitated by the community.

CONCLUSION 5 — PLATFORM ADMINISTRATIVE INVOLVEMENT — NOT SUPPORTED — HIGH CONFIDENCE

(TS//SI//NF) Platform administrators had no foreknowledge of or involvement in the incident. Post-incident content deletion by administrators is assessed as a reputational management decision and not indicative of prior knowledge or complicity.

B-11. RECOMMENDATIONS

B-REC-1 — MAINTAIN HCS COLLECTION POSTURE — PRIORITY: HIGH

(S//NF) Maintain current active HUMINT collection posture, including all three current assets. The incident and its community nexus validate the investment in HUMINT collection against this target. Recommend handler contact frequency for ASSET YELLOWJACKET be increased from monthly to biweekly for the duration of post-incident community behavioral monitoring.

B-REC-2 — SUPPORT FBI INVESTIGATION — ONGOING — PRIORITY: HIGH

(S//NF) Continue providing SIGINT technical support to FBI criminal investigation under existing MOU. Ensure all future transfers are reviewed by NSA/OGC prior to provision. If FBI requests additional historical collection data, process through standard NSA/OGC review and document in CTID dissemination log.

B-REC-3 — ACQUIRE COMMUNITY ARCHIVE MATERIAL — PRIORITY: MODERATE

(TS//HCS//NF) Authorize ASSET MOONRAT to proceed with passive acquisition of community-preserved archive of pre-incident post content (see Section B-5.2). Any material obtained to be ingested into CTID analytical holdings and shared with FBI under MOU. Handler [REDACTED] to manage operational security of acquisition attempt.

B-REC-4 — REFINE XKS ALERT THRESHOLDS — PRIORITY: MODERATE

(TS//SI//NF) Post-incident review identified that POST [RED]-05 fell below automated alert thresholds due to keyword gap. Recommend CTID/SIGDIV conduct a structured review of XKS keyword and threshold parameters for this target, with a view to reducing false-negative rate for operationally significant content. Output to be documented as a collection improvement product within 60 days.

B-REC-5 — BRIEF NCTC ON RADICALIZATION PATHWAY FINDING — PRIORITY: MODERATE

(S//NF) Provide a sanitized radicalization pathway assessment to NCTC for incorporation into its imageboard community radicalization mapping efforts. Brief should include CONCLUSIONS 3 and 4 with appropriate confidence caveats. Coordinate with NSA/CSS Public Affairs and OGC regarding any potential downstream public characterization.

B-REC-6 — UPDATE ACTOR PROFILES — PRIORITY: ROUTINE

(TS//HCS//NF) Update ANNEX D actor profiles for USERNAME-A and USERNAME-B to reflect current confidence levels, FBI investigative status, and post-incident collection. Profiles are currently dated to mid-2023 and require updating to reflect new information derived from this investigation.

B-12. DISSEMINATION AND OVERSIGHT

(U//FOUO) All dissemination of this annex is restricted to Bigot List Alpha. No portion of this annex may be shared, summarized, paraphrased, or referenced in any other document without prior written authorization from the NSA/CTID HUMINT Operations Cell Supervisor. Any downstream product derived from this annex must carry appropriate source caveats and HCS control markings.

(U//FOUO) Oversight documentation for this annex — including Bigot List Alpha membership records, access logs, transfer records, and OGC legal reviews — is maintained by the NSA/CTID Security Officer and the NSA/CSS Privacy and Civil Liberties Office. This documentation is available to the NSA Inspector General and to Congressional oversight committees with appropriate clearances upon request through established oversight channels.

B-13. ANALYTICAL CONFIDENCE SUMMARY AND CAVEATS

(U//FOUO) The following table summarizes key analytical confidence assessments in this annex for reference by downstream analysts.

ASSESSMENT QUESTION	CONFIDENCE	BASIS / NOTE
USERNAME-A = Subject of FBI investi	HIGH	SIGINT + FBI independent corrobora
Community nexus (participation)	HIGH	Multi-source corroboration
Pre-incident posts authored by USER	HIGH (Posts 05–06)	MODERATE (Posts 03–04)
Third-party foreknowledge	LOW — NOT CONFIRMED	Absence of corroborating evidence
Platform as contributing radicaliza	MODERATE	FBI BAU concurs; inherent limits o
Organized community involvement	NOT SUPPORTED — HIGH	FBI working assumption: lone actor
Admin prior knowledge or complicity	NOT SUPPORTED — HIGH	Deletion assessed as reputational
Stylometric model attribution (USER	HIGH (model output)	Pending external model validation

(U//FOUO) Analysts are reminded that confidence levels in this annex reflect the state of the evidence as of March 2024. The FBI criminal investigation is ongoing and may produce new evidence that alters these assessments. CTID/OSIB will issue supplemental reports as warranted. Any analyst who receives new information bearing on this assessment should contact the CTID HUMINT Operations Cell immediately.

B-14. PREPARED BY / REVIEW AND APPROVAL

(U//FOUO) This annex was prepared jointly by the NSA/CTID HUMINT Operations Cell and the FBI Behavioral Analysis Unit, with contributions from CTID/OSIB, CTID/SIGDIV, and CTID/DS. It has been reviewed for classification accuracy and HCS compliance by the CTID Classification Management Officer and the NSA/CSS HUMINT Operations Security Officer, and approved for Bigot List Alpha dissemination by the CTID Division Chief.

PREPARED BY (NSA):	[REDACTED] — HUMINT Operations Cell, CTID
PREPARED BY (FBI):	[REDACTED] — Behavioral Analysis Unit, FBI HQ
REVIEWED BY:	[REDACTED] — CTID Classification Management Officer
REVIEWED BY (HCS):	[REDACTED] — NSA/CSS HUMINT Operations Security Officer
APPROVED BY:	[REDACTED] — CTID Division Chief
DATE:	04 March 2024

— END OF ANNEX B — NSA-CTI-2024-0391-B/B (TS//SI//HCS//NOFORN — BIGOT LIST ALPHA)

Continue to ANNEX C: Platform Founder Biographical Assessment (TS//SI//HCS//NOFORN)
ANNEX D: Key Actor Biographical Dossiers (TS//SI//HCS//NOFORN) — BIGOT LIST ALPHA