TECHNICAL REQUIREMENTS AND SCOPE

1. PROJECT OVERVIEW

The National Forensics Agency (NFA) aims to develop OSINT tool, capable of comprehensive data collection and analysis from public sources. This initiative is driven by:

1. The need for sovereign control over intelligence gathering tools
2. Rising costs of commercial OSINT solutions
3. Increasing complexity of online data sources
4. Integration of AI in data analysis
5. Need for rapid response to emerging online threats

It is expected that a timeline and detailed technical capabilities to be provided in response to this document

2. TECHNICAL CAPABILITIES REQUIRED

2.1 Data Source Coverage

1. Social media platforms integration
2. Public records databases
3. News and media sources
4. Business registries and financial databases
5. Domain and IP intelligence
6. Dark web monitoring capabilities
7. Public government databases

2.2 Data Collection Capabilities

1. Automated web scraping
2. API integration with major platforms
3. Real-time data streaming
4. Historical data archiving
5. Metadata extraction
6. Document and image collection
7. Geolocation data gathering

2.3 Analysis Features

1. Entity recognition and linking
2. Network analysis and visualization
3. Timeline reconstruction
4. Pattern recognition
5. Sentiment analysis
6. Geographic mapping
7. Automated report generation

8. Cross-platform correlation

2.4 Technical Implementation Requirements

1. Distributed architecture for scalability
2. Real-time processing capabilities
3. Data validation and verification
4. API development for integration
5. Multi-language support
6. Data storage and indexing

3. AREAS OF RESEARCH INTEREST

3.1 Core Technologies

1. Advanced web crawling techniques
2. Data extraction methodologies
3. Natural Language Processing
4. Network analysis algorithms
5. Data visualization techniques

3.2 AI Integration

1. Machine learning for data classification
2. Automated pattern recognition
3. Entity relationship mapping
4. Predictive analysis
5. Anomaly detection
6. Language translation and analysis

3.3 Software Development

1. Scalable architecture design
2. User interface development
3. Database optimization
4. API development
5. Security implementation

4. INFORMATION REQUESTED

4.1 Research Capabilities

1. Current research projects in OSINT
2. Published works in relevant areas
3. Ongoing development projects
4. Laboratory facilities
5. Research team expertise

4.2 Technical Infrastructure

1. Computing facilities
2. Development environments
3. Testing infrastructure
4. Data storage capabilities
5. Network infrastructure

4.3 Academic Resources

1. Faculty expertise in relevant areas
2. Graduate research programs
3. Industry partnerships
4. International collaborations
5. Publication history

5. DEVELOPMENT METHODOLOGY

5.1 Expected Approach

1. Agile development methodology
2. Continuous integration/deployment
3. Regular security updates
4. Extensive testing
5. Documentation and knowledge transfer
6. Quality assurance protocols

5.2 Documentation Requirements

1. Technical documentation
2. API documentation
3. User manuals
4. Training materials
5. Standard operating procedures

6. COMPLIANCE AND STANDARDS

6.1 Required Standards

1. Data privacy compliance
2. GDPR considerations
3. Ethical data collection guidelines
4. Chain of custody requirements
5. Data integrity verification

7. INTELLECTUAL PROPERTY AND FUNDING

7.1 Intellectual Property Rights

1. All intellectual property developed under this initiative shall be the exclusive property of NFA
2. This includes but is not limited to:
   a) Source code
   b) System architecture
   c) Technical documentation
   d) Research findings
   e) Patents and innovations
   f) Methodologies and protocols
3. Partner institutions will be acknowledged in academic publications with NFA's prior approval
4. Non-disclosure agreements will be required for all participating personnel
5. Detailed budget allocation will be discussed with selected institutions
6. Regular financial audits and progress reviews will be conducted

OSINT TOOL Technical Requirements Specification Social Media Data Extraction Module

1. OVERVIEW

1.1 Purpose The social media extraction module of OSINT tool shall provide comprehensive capabilities for collecting, analyzing, and correlating data from major social media platforms including but not limited to X , Facebook, WhatsApp, TikTok, YouTube, and Instagram.

1.2 Scope This module shall enable automated collection and analysis of publicly available social media data while maintaining compliance with platform policies and legal requirements.

2. PLATFORM-SPECIFIC REQUIREMENTS

2.1 X Data Collection

- User Profile Analysis

  a) Basic information extraction (username, display name, bio, location)
  b) Profile creation date and modifications
  c) Profile picture history and analysis
  d) Account relationships (followers/following)
  e) Listed accounts and list memberships

- Tweet Analysis

  a) Historical tweet collection and archiving
  b) Media attachment collection (images, videos, GIFs)
  c) Engagement metrics (likes, retweets, replies)

d) Hashtag tracking and trending analysis
e) Geolocation data from tweets
f) Mentioned accounts and interactions
g) Tweet sentiment analysis
h) URL extraction and analysis

2.2 Facebook Data Collection

- Profile Information

  a) Public profile data extraction
  b) Friend network analysis
  c) Group memberships
  d) Page likes and follows
  e) Events participation

- Content Analysis

  a) Public posts and updates
  b) Shared media content
  c) Comment threads and reactions
  d) Tagged locations and check-ins
  e) Public stories and reels
  f) Business page information

2.3 WhatsApp Analysis (Public Sources)

- Public Group Information

  a) Group invite links monitoring
  b) Public group participant analysis
  c) Group description and rules
  d) Shared public content analysis

- Business Account Analysis

  a) Business profile information
  b) Public catalog items
  c) Business status updates
  d) Customer interaction patterns

2.4 TikTok Data Collection

- Account Analysis

  a) Profile information extraction
  b) Follower/following relationships

c) Account statistics and metrics
d) Profile verification status

- Content Analysis

a) Video content collection
b) Hashtag tracking
c) Sound and music usage patterns
d) Engagement metrics
e) Comment analysis
f) Live stream monitoring
g) Challenge participation tracking

2.5 YouTube Data Analysis

- Channel Information

a) Channel metadata extraction
b) Subscriber growth tracking
c) Platform engagement metrics
d) Channel relationships

- Content Analysis

a) Video metadata collection
b) Comment extraction and analysis
c) Playlist organization
d) Description and tag analysis
e) Caption/subtitle extraction
f) Live stream monitoring
g) Community post analysis

2.6 Instagram Data Collection

- Profile Analysis

a) Account information extraction
b) Follower/following relationships
c) Story highlights
d) Tagged content analysis
e) Business account details

- Content Collection

a) Post metadata and media
b) Story monitoring
c) IGTV content

d) Reels analysis
e) Location tagging
f) Hashtag usage patterns
g) Comment thread analysis

3. TECHNICAL IMPLEMENTATION REQUIREMENTS

3.1 Data Collection Methods

1. API Integration
   a) Official API implementation for each platform
   b) Rate limit management
   c) Authentication handling
   d) Error recovery mechanisms
2. Web Scraping Capabilities
   a) Dynamic content handling
   b) Anti-detection mechanisms
   c) Proxy management
   d) Browser fingerprint randomization
   e) CAPTCHA handling
3. Real-time Monitoring
   a) Live data stream processing
   b) Event-based triggers
   c) Alert system for specific activities
   d) Automated collection scheduling

3.2 Data Processing Features

- Content Analysis

  a) Multi-language text processing
  b) Image recognition and classification
  c) Video content analysis
  d) Audio transcription and analysis
  e) Metadata extraction and correlation
  f) Entity recognition and linking

- Network Analysis

  a) Social network mapping
  b) Influence measurement
  c) Community detection
  d) Connection pattern analysis
  e) Cross-platform correlation

3.3 Data Storage and Management

- Database Requirements

  a) Scalable storage architecture
  b) Real-time indexing
  c) Data deduplication
  d) Version control
  e) Backup mechanisms

- Data Organization

  a) Structured data schemas
  b) Relationship mapping
  c) Temporal organization
  d) Geographic indexing
  e) Platform-specific taxonomies

4. ANALYSIS AND REPORTING

4.1 Automated Analysis

- Pattern Recognition

  a) Behavioral analysis
  b) Content similarity detection
  c) Temporal patterns
  d) Geographic patterns
  e) Network patterns

- AI/ML Capabilities

  a) Sentiment analysis
  b) Topic modeling
  c) User profiling
  d) Anomaly detection
  e) Prediction modeling

4.2 Reporting Features

- Report Generation

  a) Customizable templates
  b) Multiple export formats
  c) Visual representations
  d) Timeline views
  e) Network graphs
  f) Geographic mapping

- Alert System

  a) Real-time notifications
  b) Customizable triggers
  c) Priority levels
  d) Escalation procedures
  e) Alert aggregation

5. COMPLIANCE AND SECURITY

5.1 Legal Compliance

1. Platform Terms of Service adherence
2. Data protection regulations compliance
3. Privacy law considerations
4. Ethical guidelines implementation
5. Audit trail maintenance

5.2 Security Features

1. Data encryption
2. Access control
3. User authentication
4. Activity logging
5. Secure data transmission

6. SYSTEM REQUIREMENTS

6.1 Performance Specifications

1. Minimum concurrent collections: 1000
2. Real-time processing capability
3. Maximum latency: 5 seconds
4. 99.9% system uptime
5. Scalable to handle 10TB+ of data

6.2 Integration Requirements

1. REST API support
2. Webhook implementation
3. Database compatibility
4. Export format support
5. Third-party tool integration

7. MAINTENANCE AND UPDATES

7.1 System Maintenance

1. Regular platform updates
2. API version management
3. Database optimization
4. Performance monitoring
5. Error logging and handling

7.2 Update Requirements

1. Automated update mechanisms
2. Platform change adaptation
3. New feature integration
4. Backward compatibility
5. Documentation updates

OSINT Tool Development:

PROJECT INITIATION

Project Setup

1. Sign Non-Disclosure Agreements (NDAs) for all participating personnel
2. Establish project management infrastructure and communication channels
3. Define roles, responsibilities, and reporting structure
4. **Priority Right**: Document intellectual property framework confirming NFA's exclusive ownership of all developed assets

Requirements Analysis

1. Conduct detailed requirements gathering workshops for all social media platforms
2. Document system architecture requirements and technical constraints
3. Establish data compliance and legal framework
4. Certified Check: Complete initial security requirements review
5. Create project risk register and mitigation strategies

ARCHITECTURE AND DESIGN

System Architecture

1. Design high-level and detailed system architecture
2. Define technology stack and compatibility requirements
3. Create database schema and data flow diagrams
4. Certified Check: Architecture security review by independent third party
5. Priority Right: Document NFA priority access protocols for emergency operations

Development Environment

1. Set up development, testing, and staging environments
2. Configure version control systems and code repositories
3. Establish CI/CD pipeline and automated testing framework
4. Implement secure coding standards and review processes
5. Certified Check: Verify isolation of development environment from production networks

CORE ENGINE DEVELOPMENT

Data Collection Engine

1. Develop core data extraction framework
2. Implement API integration capabilities for primary platforms
3. Create web scraping modules with anti-detection mechanisms
4. Certified Check: Verify compliance with platform Terms of Service
5. Establish rate limiting and error handling protocols

Data Storage System

1. Implement scalable database architecture
2. Develop data indexing and search capabilities
3. Create backup and recovery mechanisms
4. Certified Check: Database security assessment and penetration testing
5. Priority Right: Implement NFA-exclusive data access controls

X AND FACEBOOK MODULES

X Module

1. Develop X user profile analysis features
2. Implement tweet collection and historical archiving
3. Create hashtag tracking and trending analysis capabilities
4. **Certified Check**: X module performance testing
5. Implement metadata extraction for X content

Facebook Module

1. Develop Facebook profile data extraction
2. Create public content analysis for posts and media
3. Implement friend network and group membership analysis
4. **Certified Check**: Facebook module privacy impact assessment
5. **Priority Right**: Establish protocols for critical intelligence findings

INSTAGRAM AND WHATSAPP MODULES

Instagram Module

1. Develop Instagram profile analysis system
2. Create post, story, and IGTV content collection
3. Implement location tagging and hashtag analysis
4. **Certified Check**: Verify compliance with Instagram platform policies
5. Test cross-platform correlation with previously developed modules

WhatsApp Module

1. Implement public group information monitoring
2. Develop business account analysis capabilities
3. Create shared content analysis system
4. **Certified Check**: Legal compliance review for WhatsApp data collection
5. **Priority Right**: Define classification system for WhatsApp intelligence

TIKTOK AND YOUTUBE MODULES

TikTok Module

1. Develop TikTok account analysis system
2. Create video content collection and hashtag tracking
3. Implement engagement metrics analysis
4. **Certified Check**: Verify compliance with TikTok Terms of Service
5. Test integration with core analysis engine

YouTube Module

1. Develop YouTube channel metadata extraction
2. Create video and comment analysis capabilities
3. Implement caption/subtitle extraction features
4. **Certified Check**: Performance testing for high-volume video processing
5. **Priority Right**: Establish protocols for handling sensitive video intelligence

ANALYSIS ENGINE DEVELOPMENT

Content Analysis Features

1. Implement multi-language text processing
2. Develop image recognition and classification
3. Create entity recognition and linking system
4. **Certified Check**: Accuracy testing against benchmark datasets
5. Implement cross-platform entity correlation

Network Analysis Features

1. Develop social network mapping capabilities

2. Create influence measurement algorithms
3. Implement community detection features
4. **Certified Check**: Verify algorithm effectiveness with test networks
5. **Priority Right**: Create specialized analysis tools for NFA priority cases

AI/ML INTEGRATION

Basic AI Implementation

1. Develop sentiment analysis across all platforms
2. Create topic modeling and content classification
3. Implement behavioral pattern recognition
4. **Certified Check**: AI model accuracy and bias assessment
5. Document AI model limitations and confidence metrics

Advanced AI Features

1. Implement anomaly detection algorithms
2. Develop predictive analysis capabilities
3. Create user profiling based on cross-platform data
4. **Certified Check**: Verify AI feature compliance with ethical guidelines
5. **Priority Right**: Define NFA exclusive access to advanced AI findings

REPORTING AND ALERTING

Reporting System

1. Create customizable report templates for different use cases
2. Implement visual representations (networks, timelines, maps)
3. Develop export capabilities in multiple formats
4. **Certified Check**: Report accuracy verification with test data
5. Implement audit logging for all report generation

Alert System

1. Develop real-time notification system
2. Implement customizable alert triggers
3. Create priority levels and escalation procedures
4. **Certified Check**: Alert system reliability under stress testing
5. **Priority Right**: Configure special alert protocols for NFA priorities

SYSTEM INTEGRATION

Module Integration

1. Perform comprehensive integration of all platform modules
2. Implement cross-platform correlation features

3. Create unified user interface for all functions
4. **Certified Check**: End-to-end system integration testing
5. Document system dependencies and integration points

System Optimization

1. Perform performance optimization across all modules
2. Implement caching and request batching
3. Create system health monitoring
4. **Certified Check**: System performance under peak load conditions
5. **Priority Right**: Define resource allocation priorities for NFA operations

TESTING AND VALIDATION

Security Testing

1. Conduct comprehensive security audit
2. Perform penetration testing on all system components
3. Implement security fixes and improvements
4. **Certified Check**: Independent security assessment by third party
5. Document all security measures and residual risks

User Acceptance Testing

1. Conduct supervised testing with NFA personnel
2. Document user feedback and usability issues
3. Implement critical fixes and improvements
4. **Certified Check**: Verify system meets all functional requirements
5. **Priority Right**: Implement NFA-requested priority modifications

DEPLOYMENT AND HANDOVER

Deployment Preparation

1. Finalize all documentation and user manuals
2. Prepare production environment
3. Conduct training sessions for NFA staff
4. **Certified Check**: Pre-deployment system verification
5. Create deployment rollback plan

Final Deployment

1. Deploy to production environment
2. Complete knowledge transfer to NFA technical team
3. Deliver all source code, documentation, and materials
4. **Certified Check**: Final acceptance testing with NFA sign-off
5. **Priority Right**: Establish ongoing maintenance and support protocols with defined NFA priorities

POST-PROJECT CONSIDERATIONS

Ongoing Support

1. Regular security updates and API adaptation
2. Monthly feature enhancements based on operational feedback
3. **Certified Check**: Quarterly security and compliance reviews
4. **Priority Right**: NFA retains first-right for all enhancement requests