NIPRGPT Cybersecurity FAQ

NIPRGPT, a Generative Artificial Intelligence (GenAI) capability offered by the Department of the Air Force (DAF). This FAQ is to address both common user and IT leader questions in context to cybersecurity in the usage of the NIPRGPT system.

What is NIPRGPT and what is the intended purpose of its use?

- NIPRGPT is a comprehensive Artificial Intelligence (AI) platform featuring Retrieval Augmented Generation (RAG) that permits users to interact with a Large Language Model (LLM).

Has NIPRGPT been authorized for use?

- Yes, NIPRGPT has an Authority to Operate (ATO). This ATO is based on emplacement and artifact proof meeting requirements from the Committee on National Security Systems Instruction (CNSSI) 1253, NIST SP 800-53 security controls, AFI 17-101, and active cybersecurity mechanisms in place to protect CUI data.
    - ***What does this mean for users?*** NIPRGPT can be used for operational purposes based on data protection in place of a National Security System (NSS).
- Additionally, NIPRGPT does not have access to any system, application, or network outside of the purview or authorized system boundaries for the DoD or DAF cybersecurity regulations.

Is NIPRGPT compliant with cybersecurity and authorization requirements?

- Yes, NIPRGPT is compliant with all CNSSI 1253 for NSS, DoD, and DAF regulations and requirements. Additionally, NIPRGPT incorporates Zero-Trust (ZT) meeting DoD guidance for technical security protections and timelines.
- Independent cybersecurity assessments were conducted to ensure NIPRGPT's compliance with risk management framework security controls per CNSSI 1253 for NSS, NIST SP 800-37/53r5, DISA Container Hardening Process Guide, DISA Cloud Security Requirements Guide, DISA STIGs, DoD CNAP Reference Design, DoD Zero-Trust Reference Architecture, and supplementary documentation for qualitative and quantitative temporal assessment factors.

What is the classification of the NIPRGPT architecture, cybersecurity mechanisms, and subsequent infrastructure or programmatic details of NIPRGPT?

- The architecture, cybersecurity mechanisms, incident response, and accreditation specific details are Controlled Unclassified Information // Controlled Technical Information (CUI//CTI). As such these details must be treated appropriately per Executive Order 13556, 32 Code of Federal Regulations, Part 2002, DoD Instruction 5200.48, and others. As such, details of architecture, cybersecurity mechanisms, incident response, and accreditation specific details are not designed for public dissemination including sharing through social media, news channels, and other unclassified means.

What is the Impact Level of the NIPRGPT system and what data types are permitted to be entered into the tool?

- Impact Level 5 (IL5)
- CUI data protections are in place

What data types are NOT permitted on NIPRGPT?

- There are limitations to what types of data can be put on a system based on regulatory and protection mechanisms. These warnings are also on the NIPRGPT Terms of Use.
- The following data types are **NOT** permitted on NIPRGPT:
    - **NO** classified data (e.g., Alternate Compensatory Control Measures (ACCM), Special Access Program (SAP), Sensitive Compartmented Information (SCI), etc.)
    - **NO** International Traffic in Arms Regulations (ITAR) or export-controlled data
    - **NO** Information protected by the Privacy Act of 1974, as amended
    - **NO** Personally Identifiable Information (PII)
    - **NO** Information protected by the Health Insurance Portability and Accountability Act (HIPAA/PHI - Protected Health Information).

Are my interactions with NIPRGPT private?

- NIPRGPT is a DAF system, and users must acknowledge the U.S. Government (USG) Notice and Consent warning, during authentication into the NIPRGPT system. With this acknowledgement users consent to the following:

  By using this Information System (IS) (which includes any device attached to this IS), you consent to the following conditions:

    - *The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.*
    - *At any time, the USG may inspect and seize data stored on this IS.*
    - *Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.*

- *This IS includes security measures (e.g., authentication and access controls) to protect USG interests – not for your personal benefit or privacy.*
- *Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work products are private and confidential. See User Agreement for details.*

How is my workspace data stored?

- Workspace data is encrypted and tied to the user. Documents uploaded into a workspace are private unless you explicitly share them.

Are the encryption mechanisms on NIPRGPT approved?

- Yes, encryption mechanisms within NIPRGPT are captured in the system Authority to Operate (ATO) boundary/scope and meeting requirements of Federal Information Processing Standard (FIPS) 199, FIPS 200, FIPS 140-2 and FIPS 140-3 or higher as mandated by Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106), the Computer Security Act of 1987 (Public Law 1--0235), all DoD and CNSSI 1235.

Are my interactions with NIPRGPT and my NIPRGPT Workspace secure?

- Yes, all interactions with NIPRGPT are cryptographically isolated, logged, and audited.
- Your session and your workspace access (including document upload & query) is controlled with attribute-based controls, multifactor authentication, and enforced using non-repudiation functions, via PKI infrastructure.

How are Large Language Models (LLMs) evaluated prior to inclusion in NIPRGPT?

- Incorporation of LLMs adhere to FAR/DFAR requirements as well as cybersecurity requirements for accreditation. This includes appropriate sourcing of hardware and software components leveraged by the system. NIPRGPT has never loaded nor accessed nation state actor LLMs or systems.
- A certified DoD Red Team performed extensive tests and assessments against the NIPRGPT infrastructure and the LLMs deployed.

Who monitors & is responsible for NIPRGPT cybersecurity?

- The NIPRGPT system has overlapping cybersecurity measures for monitoring and oversight including:
  - DISA Cybersecurity Service Provider (CSSP), providing proactive monitoring, threat detection, and incident response for NIPRGPT, enhancing its security posture and reducing cyberattack risks
  - Multiple layers of continuous automated sensing and alerting for all telemetry, logs, vulnerabilities, and compliance configurations

- System technical support & operations team (engineering, system developers, subject matter experts) with ability to triage incidents within NSS security control threshold requirements for incident response
- Systems authorization team members including the Authorizing Official (AO), NIPRGPT cybersecurity personnel, and Information Systems Security Managers/Officers (ISSMs/ISSOs)

What should I do if I encounter a security issue or anomaly?

- Suspected security incidents or anomalies must be reported immediately to:

  Email: disa.columbus.eis.mbx.cols-esdna@mail.mil
  Email: disa.dscc.eis.mbx.cols-esdna@mail.mil

  General CSSP related questions can be sent to the CSSP Team at:
  Email: disa.letterkenny.j3-5-7.list.cssp@mail.mil

- Additionally, the 'Feedback & Support' feature within NIPRGPT can be used to send a message to NIPRGPT@us.af.mil with Subject Line: **NIPRGPT CYBER INCIDENT**.

Generative AI Usage Reminder: Precautions must be taken as GenAI and LLMs are assistive tools and not authoritative sources. NIPRGPT users have the responsibility for data handling and analysis results, as with other DoD information systems:

- GenAI capabilities can generate untruthful or inaccurate responses (known as 'hallucinations'). Although GenAI capabilities can save time by providing initial answers to inquiries, users are responsible for validating whether the outputs are true and accurate.
- Only GenAI capabilities with system authorizations (e.g., ATOs) approved to handle the appropriate level of sensitivity and classification levels can be used.
- Be aware that data aggregation by GenAI systems can increase data sensitivity levels. Carefully consider the cumulative effect of the data you input or share within these systems (e.g. risks of classification by compilation).

For additional regulatory and policy specific inquiries see the DAF Chief Data & Artificial Intelligence Officer (CDAO) SharePoint site Strategy, Policy, & Guidance or https://usaf.dps.mil/sites/13057/CND/SitePages/Policies-&-Standards.aspx

For a list of approved DAF AI software please see https://www.dafcio.af.mil/AI/AIX/