EBRC Engineering Biology Research Consortium

Nucleic Acid Synthesis Screening elements of EO 14292: Improving the Safety and Security of Biological Research

Compiled and edited by Rebecca Mackelprang
EBRC Director for Security Programs
June 2025

Key Points & Recommendations

- The Updated Framework (UF) on nucleic acid synthesis screening (NASS) being developed by OSTP at the direction of *Executive Order 14292: Improving the Safety and Security of Biological Research* should require recipients of federal grants and awards, through contract terms, to purchase nucleic acids from Providers who have passed a third-party assessment of baseline sequence screening capabilities by January 1, 2026.
- The UF should describe screening processes for other elements of screening (customer screening, follow-up screening, law enforcement reporting, record keeping, and cyber & information security) and require recipients of federal grants and awards to purchase nucleic acids from Providers who have issued a Declaration of Adherence to these practices by January 1, 2026.
- USG should continue to fund and support NIST and private sector coalitions working to develop measurable standards for all elements of NASS.
- USG should support the development and piloting of NASS assessment modalities, with an emphasis on enabling end-to-end stress testing by trusted third parties (see Annex I.C.).

The Engineering Biology Research Consortium (EBRC)* applauds the Trump Administration's commitment to ensuring that the United States continues to "[drive] global leadership in biotechnology, biological countermeasures, biosecurity, and health research" while recognizing the need for robust biosafety and biosecurity measures. EBRC is a non-profit, public-private partnership that works to build community to advance engineering biology research and the bioeconomy across our four focus areas, one of which is security. We are thus dedicated to serving as a resource to the Administration as it executes on *Executive Order 14292: Improving the Safety and Security of Biological Research*. Here, in Sections I-III, we provide recommendations for an enforceable framework for nucleic acid synthesis screening (NASS). Additional information on the strengths and weaknesses of screening assessment approaches is highlighted in Annex I, and Annexes II-IV suggest best practices for NASS. Comments are largely based on our engagement with the NASS community, including providers, customers, standards bodies, and biosecurity experts both in the U.S. and internationally.[1]

* The Engineering Biology Research Consortium brings engineering biology researchers and other stakeholders from industry, academia, and government together to advance engineering biology to address national and global needs. EBRC products do not necessarily reflect the direct views of all EBRC members.

I. A Common Sense Approach to Nucleic Acid Synthesis Screening (NASS)

EBRC strongly supports policy articulating "a commonsense approach [that] effectively encourages providers of synthetic nucleic acid sequences to implement comprehensive, scalable, and verifiable synthetic nucleic acid procurement screening mechanisms to minimize the risk of misuse." Given our extensive engagement and published contributions across this topic[2-4] and ongoing projects[5-7], we suggest that OSTP, as it executes on EO 14292, consider that:

- nucleic acid synthesis providers **("Providers") can only be evaluated for compliance with the Updated Framework (UF) for screening elements that are clearly defined, measurable, and for which assessment capabilities have been developed**.
- Thus, by January 2026 (or April 2026, if need be), recipients of research contracts and grant awards should be directed, with reasonable accompanying enforcement measures, to procure nucleic acids from Providers who have passed a third-party sequence screening assessment for baseline sequence screening capabilities.
- For all other screening elements (e.g., customer screening, law enforcement reporting), recipients of research contracts and grant awards should be directed, with reasonable accompanying enforcement measures, to procure nucleic acids from Providers who have issued a Declaration of Adherence to the screening processes described in the UF.
- In parallel, USG should support efforts to develop measurable standards and assessment capabilities (see Annex I) for all other screening elements.

II. Sequence Screening Standard and Assessment

Definitions of "Sequence of Concern" have been articulated by the 2023 HHS ASPR *Screening Framework Guidance for Providers and Users of Synthetic Nucleic Acids* and the 2024 OSTP *Framework for Nucleic Acid Synthesis Screening*. These definitions are sufficient for the measurement of a Provider's baseline sequence screening capabilities.

Thus, in the near term, third-party assessment should focus on sequence screening capabilities. Multiple organizations (i.e. IBBIS, MITRE, SecureDNA) are working toward the capability to assess demonstrations of baseline sequence screening capabilities, enabled by the development of a test data set by NIST.[†]

Note that current definitions of "Sequence of Concern" are imperfect and will be interpreted differently by stakeholders. To support harmonized screening, the Updated Framework should note that, for bacteria and fungi, only genes or genetic elements that have been experimentally demonstrated in scientific literature to directly endow or enhance pathogenicity should be considered a SOC, and that genes or genetic elements required for basic metabolic, growth, and reproductive functions are not considered to endow or enhance pathogenicity, even if their absence attenuates the pathogen.[8]

Note that screening assessment should avoid assessing the nuances and gray areas of the SOC definition, instead focusing on sequences that clearly meet the definition of "SOC."

In the next 18 months, the definition of a SOC should expand beyond taxonomic lists of regulated agents and organisms to reflect sequence hazard. NIST should be funded and directed to work in partnership with the private sector to enable USG to take advantage of efforts by the private sector toward this end.

[†] The NIST test data set has been evaluated as effective and in alignment with industry interpretation of current Guidance. Metrics for "pass" and "fail" have been established that industry generally supports.

III. Other elements of NASS

Other elements of the NASS process (e.g. customer screening, follow-up screening, law enforcement reporting, record retention, and cyber & information security) do not have associated measurable standards and/or, for technical, economic, or other reasons, do not yet have assessment capabilities.[‡]

Thus, the Updated Framework (UF) should direct federal funders to direct recipients of research contracts and grant awards to procure nucleic acids from Providers who have issued a Declaration of Adherence to UF screening practices. USG should encourage a third-party to host a repository of Declarations. This would help Providers ensure their Declaration was known and available, would help customers identify adherent Providers, and would help funders or others responsible for any reasonable enforcement measures.

Customer Screening, Follow-up Screening, and Law Enforcement Reporting are discussed below.

Customer Screening

Customer screening should follow the same general principles as described in the OSTP Framework and HHS Guidance. See Annex II for suggested customer screening practices.

Over the next 12 months, NIST and relevant stakeholders should be resourced to develop clear KYC standards for both customer identity and legitimacy verification. These efforts should build upon work already initiated and or completed by NIST and other stakeholders (e.g., IBBIS). Lessons could be learned and applied from the Financial Action Task Force, International Standards Organization, and others. Efforts should focus initially on domestic orders and expand to support KYC for international customers.

Follow-Up Screening

Follow-up screening should follow the same general principles described in the OSTP Framework and HHS Guidance. See Annex III for suggested follow-up screening practices.

Note that the information/documentation customers have for demonstrating legitimacy may be highly variable, making it challenging to standardize needed documents for demonstrating legitimacy. Furthermore, international customers may have very different types of documentation.

Over the next 12 months, NIST should partner with industry to develop a follow-up screening decision support guide with lists of the types of information that demonstrate legitimacy. The development of such a guide would support the development of a measurable standard.

Law Enforcement Reporting

Law enforcement reporting should follow the same general principles as described in the OSTP Framework and HHS Guidance. See Annex IV for suggested law enforcement reporting practices.

Note that anecdotally, Providers currently have very different interpretations of the types of orders and follow-up screening results that should be reported.

In the future, NIST should work with industry to incorporate reporting thresholds into any follow-up screening decision support materials.

[‡] The process and coordination of NIST and the private sector to develop a test data set for sequence screening should be emulated for other elements of screening.

Developing standards for these elements of NASS will enable improved, harmonized screening that is able to better secure the boundary between the virtual, design phase of biological research and the physical build and test phases. This will enable the United States to remain internationally competitive while appropriately safeguarding biotechnologies.

References

1. Engineering Biology Research Consortium (2025). Strengthening a Safe and Secure Nucleic Acid Synthesis Ecosystem: Outcomes of EBRC Stakeholder Engagement. Engineering Biology Research Consortium. DOI: 10.25498/E4311B
2. Engineering Biology Research Consortium (2020). HHS RFI on Review and Revision of the Screening Framework Guidance. https://ebrc.org/publications-response-to-request-for-information-on-review-and-revision-of-the-screening-framework-guidance-for-providers-of-synthetic-double-stranded-dna/
3. Engineering Biology Research Consortium Security Working Group; Compiled and edited by Becky Mackelprang (2022). Security Screening in Synthetic DNA Synthesis: Recommendations for Updated Federal Guidance. Engineering Biology Research Consortium. doi: 10.25498/E45P4V.
4. Engineering Biology Research Consortium (2022). Public Comment on Oligo Synthesis Screening. https://ebrc.org/publications-public-comment-dna-screening/
5. Engineering Biology Research Consortium (2025). Strengthening a Safe and Secure Nucleic Acid Synthesis Ecosystem: Outcomes of EBRC Stakeholder Engagement. Engineering Biology Research Consortium. DOI: 10.25498/E4311B
6. Engineering Biology Research Consortium. Stress Testing of DNA Synthesis Screening. https://ebrc.org/focus-areas-security-end-to-end-stress-testing-e2est-of-dna-synthesis-screening/
7. Engineering Biology Research Consortium. Building International Best Practices For Robust Synthetic Nucleic Acid Screening. https://ebrc.org/focus-areas-security-building-international-best-practices-for-robust-synthetic-nucleic-acid-screening/
8. Godbold et al. (2025). The Case for Limiting “Sequences of Concern” to Those with Demonstrated Pathogenic Function. *Applied Biosafety*. https://doi.org/10.1089/apb.2025.0015

Annex I: Assessment Mechanisms

We recommend that baseline sequence screening performance be evaluated by third parties through proficiency testing.

Other elements of NASS are not yet ready for third-party assessment or evaluation, as clear standards have not been defined and/or assessment capabilities have not yet been developed. Thus, it is more appropriate for USG to support and **expand standards** and **assessment development**. As it does so, it may consider the following mechanisms for assessing performance.

A. Proficiency Testing

An assessor provides a test set to a Provider. The Provider returns its screening results to the assessor. The assessor "grades" the Provider's results. If the Provider's results meet pre-determined metrics (e.g., for accuracy, recall), the Provider has passed.

- Proficiency testing for sequence screening is well under development as a result of the activities of NIST and the stakeholder community over the last 18 months. Third parties will be using the sequence data set developed by NIST to make test sets for Providers. Providers will screen the test set and be given scores for accuracy and recall. The first instances of a third-party administered sequence screening proficiency test should take place in the coming weeks.
- This same approach could be used with customer screening once customer screening standards are sufficiently articulated. Instead of a test set of sequences, a third party could provide a test set of sequence and customer orders for a provider to put through their system. With appropriate attention and resources to NIST and the stakeholder community, this could be accomplished in 12-18 months. The NIST Standard Guide (see page 59) and new guides from IBBIS could be further developed, refined, and tested for this purpose.

Proficiency testing strengths:

- Determines if a Provider has screening capabilities that demonstrate a given level of performance.

Proficiency testing weaknesses:

- Performance under real-world circumstances is not evaluated.
- No insight into Provider internal practices or decision-making is gained.
- Follow-up screening and reporting cannot be assessed through this unblinded approach.
- This approach does not assess record keeping, cybersecurity, or other elements of NASS that may be in the Updated Framework.

B. Auditing:

A third party is given access to a Provider's process and records and determines if past decision-making and current processes align with standards.

- In NASS, this would involve a third party paid to visit a Provider and gain access to their systems, records, and processes. It would take some time to develop the appropriate scope for an audit, but some third parties, such as MITRE, are well-positioned to do this.

Auditing strengths:

- Only approach where all elements of NASS (e.g., including cybersecurity and record keeping) can be assessed.
- Auditing works well in other industries and could be used in place of proficiency testing.

- It should yield insight into real-world decision-making by Providers (although it does not directly assess this).

Auditing weaknesses:

- Requires Providers to give significant access to private information to third parties, which they may be reluctant to do without incentivization or requirements.
- Requires clear articulation of standards and agreement on the implementation of those standards between Provider, auditor, and the issuer of standards.
- Potentially expensive for Providers, though generally not cost prohibitive.
- An understanding of Provider practice is based entirely on the fidelity of their policies and record-keeping.

C. Stress Testing:

Orders are placed by a third party through regular Provider order streams. By ordering a range of sequences through different customer profiles, and through engagement with Providers during follow-up screening, the third party can gain insight into how Providers perform in real-world scenarios.

- EBRC is conducting a stress testing exercise for nucleic acid synthesis providers. Early results will be available soon.
- If USG finds this approach useful, it should designate an office or USG representative to engage with third parties developing such tests who can endorse and/or otherwise support such efforts.

Stress testing strengths:

- Provider performance is evaluated in a real-world circumstance.
- Changes to Provider performance can be evaluated over time.
- Particularly useful for benchmarking.

Stress testing weaknesses:

- The logistics (e.g., payment methods, shipping addresses, customer names, customer businesses, etc) can be challenging to set up and would benefit from government support, endorsement, or other.
- To conduct end-to-end stress testing, the ultimate outcome of some orders could result in reporting to the FBI. Consistent and reasonable assurances from the FBI as to the implications of this are needed to protect participants and to avoid wasting FBI agents' valuable time.

Given these considerations, proficiency testing should be implemented for sequence screening in the coming months. Results and output of stress testing efforts (such as those from EBRC) should be considered by USG. If valuable, USG should consider ways it can facilitate such efforts in the future. Finally, USG should provide funding to an entity to determine what auditing would entail and estimate the associated expenses for Providers.

Annex II: Suggested UF Customer Screening Processes

Customer identity should be verified for all orders, and customer legitimacy should be verified for all orders containing SOCs. Providers should be encouraged to ask customers at the time of ordering if their order is known to contain a SOC. If “yes,” information that verifies legitimacy can be provided upfront, easing and expediting the screening process for customers and providers.

1. Providers should verify the identity of all new customers through at least one mechanism, e.g. through email address or telephone number verification.
2. Each time a customer attempts to place an order, Providers should ask the customer:
    a. If their order contains a SOC (with appropriate explanation/definition of “SOC").
        i. If the customer answers “yes,” the Provider should provide field(s) for the entry of information that demonstrates customer legitimacy (see “Follow-up Screening”).
    b. If the customer is the intended “End-User” of the SOC.
        i. If “no,” and if the order does contain a SOC:
            1. the customer or end-user must provide the Provider with information to demonstrate end-user legitimacy; or
            2. the customer must have processes in place to establish the legitimacy of the end user (e.g., if the customer is a distributor).
3. After an order is successfully placed, but before it is produced, Providers should verify that the shipping address is appropriate for the ordered sequence.
4. At the time of account creation, the customer’s name and the customer’s country and institution should be screened for inclusion on any denied parties lists. Additionally, any customer placing an order should be screened for inclusion on such lists if they have not been screened in the last three months. If found on a watch list, the order must be denied.

Annex III: Suggested UF Follow-up Screening Processes

When an order contains a SOC, Providers should conduct follow-up screening. Follow-up screening should consider the legitimacy of a customer and their institution for the given sequence ordered (The previous OSTP Framework suggested types of information that may be useful in determining legitimacy.[§]). When a customer is not the end-user, the end-user’s legitimacy should also be demonstrated.

1. Customers who declare that their order contains a SOC during purchasing, and provide documentation of legitimacy, may bypass follow-up screening.
2. If such documentation is not provided when the order is placed, follow-up screening:
    a. may necessitate direct follow-up with a customer.
    b. may be satisfied through the identification of publicly available information that demonstrates legitimacy for the sequence in question.
3. If a Provider is unable to verify legitimacy, the Provider should not fulfill (deny / reject) the order.

[§] Information that may demonstrate legitimacy include “proposed end user of the order, institutional or corporate affiliation (if applicable), the name of a biosafety officer (if available), documentation of internal review and approval of the research, evidence provided by the recipient’s Responsible Official that the recipient is registered with the Federal Select Agent Program (FSAP) or Statement by Ultimate Consignee and Purchaser (i.e., a completed BIS-711 form, if applicable), other evidence of a legitimate research or training program (e.g., publication history, researcher persistent identifiers such as ORCID, business licenses, grant numbers, research plan) or other legitimate use (e.g., diagnostic test development or manufacture).”

Annex IV: Suggested UF Law Enforcement Reporting Processes

Orders that are particularly concerning or for which concerns cannot be allayed may warrant law enforcement reporting.

1. Providers should maintain a relationship with local FBI Weapons of Mass Destruction Coordinator(s).
2. Providers should report denied orders to their local FBI WMD Coordinator when:
    a. Follow-up screening does not resolve concerns about the order, AND
    b. There is reason to believe a customer may intentionally or inadvertently violate U.S. laws or regulations.