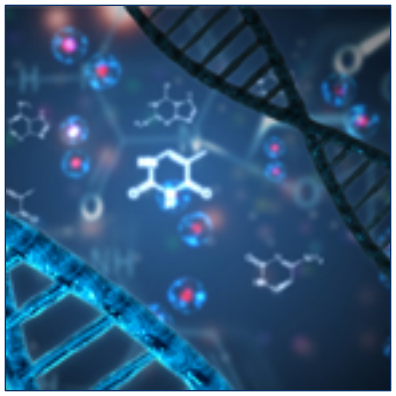
U.S. Department of Health & Human Services

Administration for Strategic Preparedness and Response

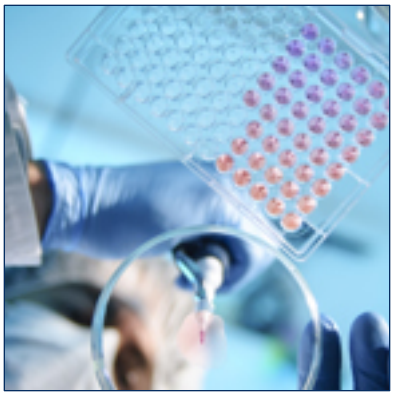
Companion Guide to Assist in Implementing the Recommendations of the *Screening Framework Guidance*

for Providers and Users of Synthetic Nucleic Acids

October 2023



ASPR



aspr.hhs.gov

Companion Guide to Assist in Implementing the Recommendations of the *Screening Framework Guidance for Providers and Users of Synthetic Nucleic Acids*

The *Screening Framework Guidance for Providers and Users of Synthetic Nucleic Acids* (or Guidance) has been issued by the Department of Health and Human Services (HHS) to assist all entities involved in the provision, use, and transfer of synthetic nucleic acids with developing best practices for screening Sequences of Concern (SOCs) in synthetic nucleic acid orders and for mitigating risks associated with those sequences. The Guidance includes, as a starting point, the definition of SOCs in the prior HHS guidance issued in 2010 (*Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA*), i.e., sequences associated with agents regulated by the Federal Select Agent Program (FSAP) or the Commerce Control List (CCL). To address concerns that have emerged with advances in synthetic biology since 2010, the Guidance recommends expanding this definition to sequences that contribute to pathogenicity or toxicity, whether from regulated agents (i.e., by FSAP or CCL) or unregulated agents – as soon as it is practical to do so. To ensure that synthetic genetic materials containing SOCs are distributed and used responsibly, the Guidance also recommends that customers (i.e., principal users and end users), providers, and third-party vendors verify the legitimacy of each recipient of nucleic acids containing SOCs – and that all parties maintain records of SOC transfers. The Guidance also recommends that manufacturers of benchtop nucleic acid synthesis equipment identify SOCs in nucleic acids prior to their synthesis and verify the legitimacy of their customers. This Companion Guide includes additional information including examples of potential scenarios that are intended to assist customers, providers, and manufacturers in implementing the recommendations in the Guidance.

Implementing Nucleic Acid Screening Mechanisms by Providers

Sequence Screening Protocol

Providers of all capacities should develop a well-documented sequence screening protocol and provide regular training on the protocol to ensure employees understand and follow it. A number of resources are available to meet the baseline recommendations outlined in the Guidance, including those from the National Center for Biotechnology Information.[1] Industry leaders and relevant industry consortium(ia) are encouraged to, wherever possible and appropriate, share best practices and methodologies for sequence screening.

Providers of synthetic nucleic acids should periodically test and measure the effectiveness of their sequence screening processes, protocols, and tools. This can be accomplished through internal quality control and quality assurance programs that provide metrics for effectiveness, or by working with external partners to validate screening accuracy. Providers of synthetic nucleic acids and manufacturers of benchtop nucleic acid synthesis equipment should consider periodically conducting penetration testing of their screening mechanisms, both to ensure that their cybersecurity standards are sufficient to protect the integrity of customer data, and to ensure that their screening mechanism is able to identify SOCs.

Record Keeping

Providers, third-party vendors, and manufacturers should retain the following types of records for a minimum of three years, or longer (e.g., eight years) if it does not pose an undue burden on their operations:

- Records of Customer orders including the following information: Customer information (point-of contact name, organization, address, email, and phone number), sequences requested including the vector used (if available), and order information (date placed and shipped, shipping address, receiver name);
- Records of protocols for sequence screening and for determining whether a sequence hit, or match, qualifies as a SOC;
- Records of screening documentation of all sequence alignment matches or hits, even if the order was deemed acceptable;
- Records of any follow-up screening, regardless of whether the order was ultimately filled; and
- The ultimate disposition of any SOC orders, with documentation of reasoning for final decision (fulfill vs deny).

These record retention times are also recommended for information regarding transfers, especially for those containing SOCs, and may be helpful in any investigation if potential misuse is suspected.

[1] https://www.ncbi.nlm.nih.gov/

Cybersecurity

Providers should aim to ensure security and integrity of their operations, including protecting against malign use, and guarding the intellectual property of their customers and the integrity of their internal SOC-screening process and database. Providers should recognize cybersecurity vulnerabilities exist and take active measures consistent with best practices and standards.[2] These measures should also protect the identity of customers whose orders are identified as containing SOCs and should be evaluated using cybersecurity risk management processes.

Manufacturers of benchtop devices should recognize the potential for malign use of this technology and aim to ensure their ability to verify the identities of customers, as well as aim to ensure the secure architecture, operation, trust, validation, and cyber incident response processes for their operations. Manufacturers should aim to ensure that their cybersecurity practices protect the intellectual property and identity of users and the SOC-screening process and database. In implementing these recommendations, manufacturers should refer to the Cybersecurity Framework Guide[3] from the National Institute of Standards and Technology (NIST) as well as other industry best practices and standards for cyber and physical security. Providers and manufacturers should also refer to NIST-published guidance for implementing critical software security measures and NIST-published guidelines for vendors,[4] which outline minimum standards for security testing their software source code and databases.

[2] Standards should align with the Presidential Executive Order 14028 on Improving the Nation's Cybersecurity (issued May 12, 2021) and the Cybersecurity Enhancement Act of 2014
[3] https://www.nist.gov/cyberframework
[4] https://www.nist.gov/cybersecurity

Verifying Legitimacy

Criteria for Verifying Legitimacy

Providers and manufacturers should verify the legitimacy of potential customers when it is determined that their synthetic nucleic acid order contains any SOC or when they are purchasing benchtop nucleic acid synthesis equipment that is capable of producing synthetic nucleic acids containing SOCs. Customers or end users who distribute synthetic nucleic acids containing SOCs to new end users (e.g., colleagues or collaborators) or distribute benchtop synthesis equipment capable of producing synthetic nucleic acids containing SOCs to new users (e.g., through resale), should also consider the details of all recipients to determine that they have a legitimate use (see below). In verifying legitimacy, other concerning details may emerge as "red flags" that could result in a need for follow-up with the customer to address these concerns (see the Red Flags for Verifying Legitimacy section).

It is important to note that the same criteria should be applied in verifying the legitimacy of customers ordering synthetic nucleic acids containing SOCs, end-users to whom these materials may be transferred, and users making synthetic nucleic acids containing SOCs with benchtop nucleic acid synthesizers. The latter case may be best addressed by establishing authentication criteria for individuals who have been verified as legitimate users for synthesizing SOCs. Institutions may also assist in aiming to ensure that only users whose legitimacy has been verified are able to use benchtop nucleic acid synthesis equipment to produce materials containing SOCs. It may be possible, for instance: 1) to restrict access to spaces where these devices are stored and used such that only legitimate users may access them; 2) to restrict logins for these machines to users whose legitimacy to synthesize SOCs has been verified; or 3) to operate a core facility where the user's legitimacy has been verified and where the legitimacy of the individual requesting nucleic acids containing SOCs is verified – if SOCs are present in the request.

Different types of information may be helpful in verifying legitimacy for accessing synthetic nucleic acids containing SOCs. Some types of information by themselves may verify legitimacy (e.g., documentation of internal review and approval of the project/research, evidence provided by the recipient's Responsible Official [RO] that the recipient is registered with FSAP, or for international orders, a completed BIS-711 form).[5] Other types of information can be used together to verify legitimacy (e.g., institutional or corporate affiliation and name of an institutional biosafety officer, or publication history and research plan). Verification of user legitimacy should include collection and review of one or more of the following information:

- Proposed end-use of the order;
- Institutional or corporate affiliation;

[5] For international orders only: https://www.bis.doc.gov/index.php/documents/just-licensing-forms/803-bis-711-statement-by-ultimate-consignee-and-purchaser-1/file

- Name of the institutional biosafety officer;
- Documentation of internal review and approval of the project/research, such as by an Institutional Biosafety Committee (IBC);
- Evidence provided by the recipient's Responsible Official (RO) that the recipient is registered with FSAP;
- Statement by Ultimate Consignee and Purchaser (i.e., a completed BIS-711 form);[5]
- Publication history;
- Open Researcher and Contributor Identifier (ORCID);[6]
- Business license(s);
- Grant number(s);
- Research plan; and
- Other legitimate use (e.g., diagnostic test development or manufacture).

In verifying legitimacy, providers should avoid the violation of personal privacy. Providers should focus on professional, not personal, information except for personal information that is necessary to establish a unique individual user identity to authenticate each recipient.

Use Cases for Verifying Legitimacy

The following narratives are intended to illustrate how providers, manufacturers, customers, and end-users can work together to aim to ensure materials containing SOCs are transferred only to legitimate members of the scientific community. These are not fully inclusive of the possible types of customers or end-users but are meant to illustrate how the Guidance's recommendations for establishing legitimacy may be implemented.

Use Case 1: Customer from a U.S. College or University

A Principal Investigator (PI) from a well-known domestic university research campus places an order with a synthetic nucleic acid provider for double-stranded DNA (dsDNA) that includes several fragments containing sequences that are 200 basepairs (bp) or longer encoding portions of the envelope protein from Ebola virus, an FSAP-regulated viral pathogen.[7] Having identified that the order contains a SOC, the company should determine whether the customer has a legitimate use for the materials, if the customer has not preemptively provided such information. Since the sequence is from a pathogen regulated by FSAP, this could include verification from their RO of FSAP registration (note that registration is not required for most work with complete genomic sequences from agents regulated by FSAP – only those from positive-stranded RNA

[6] Open Researcher and Contributor Identifier (https://orcid.org/)
[7] Or 50 nt or longer within three years of publication of the *Screening Framework Guidance for Providers and Users of Synthetic Nucleic Acids*

viruses and certain double strand DNA viruses that utilize host polymerases and contain nucleic acids that can produce infectious forms of the viruses), institutional approval for the proposed experiments, and other evidence of a legitimate research program – such as a grant number or publication history. If no preemptive information has been provided, then the provider should follow up with the customer to obtain this verification of legitimacy. Until sufficient information about the legitimacy is received and reviewed by the provider, the order should remain pending.

Use Case 2: Customer from an International Private Institution Doing Biological Research

A Laboratory Director who works at a pharmaceutical company outside the U.S. places an order with a U.S.-based synthetic nucleic acid provider for single-stranded DNA (ssDNA) that includes multiple 50 nucleotide (nt) sections that are unique to a verotoxin-producing species of *Escherichia coli* – which is included in the CCL. Having identified that the order contains SOC and that the SOCs are from an agent that is regulated, the company reviews the order and determines that an export license is required. The provider first consults the Department of Commerce's Consolidated Screening List to determine whether the Laboratory Director or the international firm are subject to any U.S. export restrictions.[8] Seeing that there are no restrictions and noticing that the Director did not preemptively provide a Statement by the Ultimate Consignee and Purchaser, the provider asks the company to complete one (i.e., a BIS-711 form). The provider also asks for additional information about the intended end-use for the order. The provider determines that the stated end-use appears to be a legitimate research purpose and receives a copy of the BIS form from the Director. Using all the information they have gathered thus far; the provider applies for an export license with the Department of Commerce. Having satisfied their concerns about legitimacy and receiving the license, they decide to fulfill the order.

Use Case 3: Customer Not Affiliated with Any Private or Public Institution

A DIY bio enthusiast from the U.S. – who is not affiliated with any private or public institution – places an order with a synthetic nucleic acid provider to be delivered to her residential address for hundreds of short ssDNA molecules between 15 nt and 30 nt in length. While none of these individual sequences constitutes a SOC, when the provider does an ungapped alignment of all the constituents of the order, two SOCs longer than 200 bp encoding the capsid protein of plum pox virus are identified.[9] The provider also notices that these constituents could be ligated into a dsDNA molecule (i.e., appropriate 3' and 5' overhangs that would allow for sequential ligation to form SOCs). Since the SOCs that could be formed from these subunits are not from a regulated agent, the provider reaches out to the DIY bio enthusiast for information about her intended use for these nucleic acids.

[8] https://www.trade.gov/consolidated-screening-list

[9] Or 50 bp or longer within three years of publication of the *Screening Framework Guidance for Providers and Users of Synthetic Nucleic Acids*

When contacted about the presence of SOC subunits in the order, the customer reports being unaware of them, as the ssDNA sequences had been generated to populate a microarray for experiments to develop an efficient and stable biological data storage mechanism. The provider offers to supply just the components of the order that do not include the SOC subunits, if the customer cannot provide more details about their legitimate use. The DIY bio enthusiast follows up with details about the research plan, multiple peer-reviewed journal articles describing their work investigating DIY bio solutions for data storage, and a newspaper clipping about their participation in last year's iGEM Jamboree. This information satisfies the provider's concerns about the legitimacy of the research program, and the order is fulfilled in its entirety.

Use Case 4: Customer at an U.S. Academic Institution Ordering Benchtop Nucleic Acid Synthesis Equipment

A Postdoctoral Fellow (postdoc) at a U.S. academic institution has been tasked with setting up an in-house nucleic acid synthesis capability in their molecular virology laboratory. The postdoc places an order for a benchtop nucleic acid synthesizer online and preemptively provides information about their research program to establish its legitimacy and conveys that the laboratory intends to register several user accounts on the device – all of which will be reviewed and approved by the PI and institution so that they should be capable of synthesizing SOCs. On receiving the order, the manufacturer of the equipment quickly determines that this is likely a legitimate transaction but follows up with the postdoc, who works with the PI to provide information about the institution's policies regarding authorized access to these devices. The postdoc confirms that the PI's laboratory staff intend to follow their institutional policy requiring that these devices are only accessed by members of the research staff. The manufacturer decides to fulfill the order and works with the postdoc, the PI and the institution to establish secure user accounts for staff, to ensure that the device is installed in a manner that allows submissions to be screened for SOCs, and to verify the legitimacy of user accounts that are authorized to synthesize nucleic acids containing SOCs. The manufacturer also refers the postdoc and PI to the Guidance, highlighting the recommendations about preventing unauthorized use of these devices, and proper handling and tracking of SOCs if they are synthesized.

Use Case 5: Customer Transfers Synthetic Nucleic Acids Containing SOCs to a Collaborator

A U.S.-based microbiology PI has been working for several years with synthetic genetic constructs that convey toxicity to an otherwise harmless fungus that is endemic in several species of arthropods. After a conference presentation the PI is approached by a new colleague – whose publications are well-known – inquiring about the molecular mechanism used to express the toxins in the fungal model of arthropod control. Upon returning from the conference, the PI reaches out to the new colleague to ask if they would like to receive a sample of the constructs discussed during the conference presentation. The new colleague accepts and provides a home address in another U.S. city. Since the PI knows that these constructs contain SOCs, and is uncomfortable with sending these materials to a home address, the PI follows up asking for an explanation. The PI's new colleague explains that they are moving to a new university and will

be continuing work shortly. The PI sees on the website of the new university that the new colleague has been hired to chair their Mycology Department. Relieved that all appears to be in order, the PI sends a congratulatory note and asks for the address of the new laboratory. The PI files a record of the transfer at their institution, and sends the constructs to the new laboratory address provided along with a material transfer agreement, if this mechanism is in place at their institution. The PI also includes a note asking that if the provided materials are to be transferred to anyone else, they should be made aware that the constructs were built from synthetic nucleic acids containing SOCs; legitimate use should be verified before transferring the materials; and records of any transfers should be maintained for a minimum of three years.

Use Case 6: Customer Purchases Sole-Use Reagents from a Manufacturer of Benchtop Nucleic Acid Synthesis Devices

The Director of a core nucleic acid synthesis facility at a U.S. pharmaceutical company is running low on reagents for benchtop nucleic acid synthesis equipment that has been in operation in his facility since 2016. The Director places an order for reagents with the manufacturer, which is the sole source of supplies for the benchtop synthesizer equipment. The manufacturer had not screened this customer or the institution for their legitimacy when it sold them the equipment almost a decade ago, and they are aware that the Guidance recommends only providing these sole-use reagents to customers whose legitimacy has been verified. They ask the Director to provide some information about the core facility and about its screening policy to verify the legitimacy of users seeking to synthesize SOCs. The Director follows up with a link to the core facility's website, which includes their policy on only providing SOCs to customers whose legitimacy has been verified. That satisfies the questions raised by the manufacturer, who decides to fulfill the order.

Use Case 7: Customer Orders Viral Vector Containing SOC from a Private U.S. Citizen.

A U.S.-based microbiology PI, who also sells recombinant adeno-associated viral (AAV) vectors as an entrepreneurial venture, receives an order for a recombinant AAV vector containing a full-length spider gene known to have hemolytic toxicity. As the PI is aware that the reformulation of this SOC gene into the AAV will result in a product containing a SOC, the PI asks for some information about the researcher ordering the recombinant AAV and their research program. The PI's customer follows up with some publications from their research program and describes the use as testing small molecule therapies against hemolytic toxins *in-vivo*. Comfortable with the legitimacy of the customer, the PI places an order with their university's core nucleic acid synthesis facility and starts the process of producing the AAV product. The PI preemptively lets the core facility know that the order contains a SOC, and the core facility easily verifies the PI's legitimacy as a well-known researcher on campus. When sending the recombinant AAV to the customer, the PI lets them know that if the materials are to be transferred to anyone else, they should be aware that the AAV was constructed from synthetic nucleic acids containing SOCs, and that records of those transfers should be kept for a minimum of three years. Finally, the PI files a record of the order with their institutional biosafety officer.

Red Flags for Verifying Legitimacy

In reviewing the information provided by recipients of synthetic nucleic acids containing SOCs or of benchtop nucleic acid synthesizers capable of making nucleic acids containing SOCs, individuals or entities transferring these materials should take into account any circumstances in the proposed transaction that may indicate that the materials may be intended for an inappropriate end-use, customer, or destination. These are known as "red flags." The following is an illustrative list of indicators that can help in identifying suspicious transactions involving synthetic nucleic acids containing SOCs or benchtop nucleic acid synthesizers:

- A recipient whose identity is not clear, who appears evasive about their identity or affiliations, or whose information cannot be confirmed or verified (e.g., addresses do not match, company name given is not that of a legitimate company, no information can be found about the company, cannot be located in trade directories, etc.);
- A recipient who would not be expected, in the course of their normal business, to place such an order (e.g., no connection to life science research or biotechnology, or no requirement for nucleic acid synthesis services);
- A recipient whose proposed use of the materials does not match their reported job or institutional affiliation;
- A recipient that requests unusual labeling or shipping procedures (e.g., requests to misidentify the goods on the packaging, or requests to change the recipient's name after the order is placed, but before it is shipped);
- A recipient proposing an unusual method of payment (e.g., arranging payment in cash, personal credit card or through a non-bank third party) or offering to pay using unusually favorable payment terms, such as a willingness to pay a higher-than-expected price;
- A recipient that requests unusual confidentiality conditions regarding the order, particularly with respect to the final destination or the destruction of transaction records; or
- A recipient that requests the order be sent to what appears to be an address without a legitimate biomedical business or research justification for the location (e.g., a residential address).

If a review of customer information reveals one or more "red flags", providers should conduct a follow-up screening. If providers' concerns are not alleviated through follow-up screening, they should not fulfill the order, and should contact their FBI Field Office's Weapons of Mass Destruction (WMD) Coordinator.

Scenarios Addressing Red Flags

The following short narratives may help entities transferring synthetic nucleic acids that contain SOCs to understand their roles in ensuring the safe use of these materials in response to "red flags." In such circumstances, the provider or manufacturer should contact the nearest FBI Field Office's WMD Coordinator and/or follow up with DOC, as appropriate. The WMD Coordinator

can be reached by contacting the local FBI Field Office and asking to be connected to the FBI WMD Coordinator.

1. Provider receives a synthetic nucleic acid order, and a suspicious customer is identified during customer screening. Follow-up screening does not resolve the concerns.

2. A principal user receives a request from another scientist for a synthetic nucleic acid order that contains SOCs that are from a biological select agent or toxin. The principal user should request evidence that the scientist has an institutionally-approved protocol, a grant number associated with the project that justifies need, a description of a legitimate research program, or confirmation of FSAP registration from the institution's RO (note that registration is not required for most work with complete genomic sequences from agents regulated by FSAP – only those from positive-stranded RNA viruses). However, the scientist is unable to provide any evidence of legitimate use as described above, and the principal user suspects malintent.

3. A provider receives a synthetic nucleic acid order that incorporates a SOC that does not come from a biological select agent or toxin. Follow-up screening reveals that the university that they claim to be affiliated with has no record of them, or – if there is a record of employment – the job they hold should not involve the purchasing or use of synthetic nucleic acids. As such, a legitimate purpose cannot be established for the order.

4. Provider receives an international synthetic nucleic acid order from a customer who is listed on one or more restricted lists, which prohibits the fulfillment of the order.

5. Manufacturer receives an order for a benchtop nucleic acid synthesis device from a customer using a residential address for shipping. On follow-up, the manufacturer determines that there is a construction and remodeling business listed at the address as well. When the manufacturer follows up about the delivery address, the customer is unresponsive and evasive about their legitimate research interest for using the device.

6. A manufacturer receives an order for a benchtop nucleic acid synthesis device from a customer who is only willing to provide payment in the form of cryptocurrency. When the manufacturer follows up to establish the identity of the customer, evasive or misleading responses indicate that the customer is attempting to remain anonymous.

Compliance with Export Administration Regulations

Summary of Export Administration Regulations (EAR)

The Department of Commerce's Bureau of Industry and Security (BIS) administers the Export Administration Regulations (EAR), pursuant to the Export Control Reform Act (ECRA) of 2018. The EAR regulates export, re-export and transfers of dual-use items for both physical objects and intellectual property. Dual-use items are those that have commercial use as well as the potential for use in military applications.

Export Control Classification Number (ECCN) 1C353 on the CCL, controls genetic elements or genetically modified organisms for all biological agents and toxins that are specific to pathogens and toxins listed in ECCNs 1C351 and 1C354.[10] These pathogens and toxins have been identified by the Australia Group, a multilateral forum consisting of 42 participating countries and the European Union, that maintain export controls on a list of chemicals, biological agents, and related equipment and technology that could be used in a chemical or biological weapons program.[11] Although the pathogens and toxins listed on the CCL and Biological Select Agents and Toxins list are similar, providers of synthetic nucleic acids must consult the CCL prior to exporting a listed SOC. If an export license is needed for the transaction, it is the responsibility of the exporter to apply for the license from BIS.

It should be noted that some domestic transfers of CCL-listed "technology" associated with "development" or "production" of genetic elements constitute an export if the materials are provided to a foreign national. This includes "technology" transfer to all foreign nationals who are in the U.S., including tourists, students, business people, scholars, researchers, technical experts, salespeople, military personnel, diplomats, etc. Simple "use" of a CCL-listed SOC does not necessarily provide a technology transfer or a need for a deemed export license. However, sharing of "production" and "development" information with a foreign person in the U.S. would. For such deemed exports, please see the FAQs on the BIS website.[12]

[10] https://www.bis.doc.gov/index.php/documents/regulations-docs/2332-category-1-materials-chemicals-microorganisms-and-toxins-4/file
[11] https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/human_animal_pathogens.html
[12] https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports/deemed-exports-faqs