Section I

[X] New Attestation

[ ] Attestation Following Extension or Waiver

[ ] Revised Attestation

Type of Attestation:

[ ] Company-wide

[X] Individual Product

[ ] Multiple Products or Specific Product Version(s) (please provide complete list)

If this attestation is for an individual product, multiple products, or product line, provide the software name, version number, and release/publish date to which this attestation applies. Additional pages can be attached to this attestation if more lines are needed:

Product(s) Name	Version Number (if applicable)	Release/Publish Date (if applicable)
FLA5120N12	2B	2023-05-24

For the above specified software, this form does not cover any components of that software that fall into the following categories:

1. Software developed by Federal agencies;
2. Open source software that is freely and directly obtained directly by a Federal agency; or
3. Software that is freely obtained and publicly available.

Note: In signing this attestation, software producers are attesting to adhering to the secure software development practices outlined in Section III.

1. Software Producer Information

Company Name: 'Weyland-Yutani Corp'
Address: 'Mars'
City: 'Gotham'
State or Province: 'Bavaria'
Postal Code: 24604
Country: 'Bin Chilling'
Email: 'weylandyutani.corp'

2. Primary Contact for this Document and Related

Information (may be an individual, role, or group):

Name: 'Yor Briar'
Title: 'Thorn Princess'
Contact Address: 'westalis'
Phone Number: 666
Email: 'thorn@strix.org'

Section III

Attestation and Signature

On behalf of the above-specified company, I attest that [software producer] presently makes consistent use of the following practices, derived from the secure software development framework (SSDF),4 in developing the software identified in Section I:

1) The software is developed and built in secure environments. Those environments are secured by the following actions, at a minimum:

a) Separating and protecting each environment involved in developing and building software;

b) Regularly logging, monitoring, and auditing trust relationships used for authorization and access:

i) to any software development and build environments; and

ii) among components within each environment;

c) Enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software in a manner that minimizes security risk;

d) Taking consistent and reasonable steps to document, as well as minimize use or inclusion of software products that create undue risk within the environments used to develop and build software;

e) Encrypting sensitive data, such as credentials, to the extent practicable and based on risk;

f) Implementing defensive cybersecurity practices, including continuous monitoring of operations and alerts and, as necessary, responding to suspected and confirmed cyber incidents;

2) The software producer has made a good-faith effort to maintain trusted source code supply chains by employing automated tools or comparable processes to address the security of internal code and third-party components and manage related vulnerabilities;

3) The software producer maintains provenance for internal code and third-party components incorporated into the software;

4) The software producer employs automated tools or comparable processes that check for security vulnerabilities. In addition:

a) The software producer operates these processes on an ongoing basis and, at a minimum, prior to product, version, or update releases;

b) The software producer has a policy or process to address discovered security vulnerabilities prior to product release; and

c) The software producer operates a vulnerability disclosure program and accepts, reviews, and addresses disclosed software vulnerabilities in a timely fashion and according to any timelines specified in the vulnerability disclosure program or applicable policies.

[X] To the best of my knowledge, I attest that all requirements outlined above are consistently maintained and satisfied. I further attest the company will notify all impacted agencies if conformance to any element of this attestation is no longer valid.