ThermoFisher SCIENTIFIC

The world leader in serving science

Dear Executive Director Byrd and Members of the ASCLD Board,

Thank you for helping ensure the forensic science community has clear information about the recently identified concern involving a potential risk related to certain electronic DNA data files. We share ASCLD's commitment to helping forensic laboratories maintain the integrity and reliability of their DNA analysis workflows.

As outlined in our security bulletin, Thermo Fisher Scientific recommends that laboratories evaluate current IT security measures alongside other established laboratory procedures and in alignment with your organization's security measures and policies. Risk mitigating controls can include maintaining file security for files generated by the instrumentation throughout the analysis workflow, storing generated files on encrypted, password-protected storage media, restricting access of generated files to authorized personnel only and leveraging firewall rules and network access control lists (NACLs) to limit internet connectivity to only trusted sources.

In addition, Thermo Fisher Scientific has released security enhancements to further reduce the potential risk for supported versions of the affected Applied Biosystems™ Data Collection and GeneMapper™ ID-X software. These updates include digital signature capabilities to add an extra layer of protection that, moving forward, will help customers verify that data files have not been modified. We are not aware of any customer data files that have been compromised through exploitation of this potential vulnerability.

We also appreciate ASCLD's recommendation regarding legacy software. Software that has reached the end of its supported lifecycle can present unique technical and validation challenges. In accordance with our software lifecycle management practices, security updates are being provided for actively supported versions of Applied Biosystems™ Data Collection and GeneMapper™ ID-X software. We will not be developing security updates for legacy, discontinued versions because, in many cases, their underlying architecture, operating system dependencies and third-party components cannot be retrofitted with modern security protections without introducing additional quality, validation and cybersecurity risks.

For laboratories that continue to operate legacy software, we recommend the IT security risk-mitigation measures outlined above and in our security bulletin, if they are not already

in place. These IT security best practices remain the primary method for protecting data integrity across laboratory workflows.

We will also continue to provide application usage guidance for legacy software, where possible, while development support—including new functionality, compatibility updates and security patches—has ended for discontinued versions.

We appreciate ASCLD's leadership and welcome continued dialogue about how we can best support the forensic science community. Additional information, including affected software, available updates and recommended security measures, is available in our security bulletin.