SOUTH DAKOTA
DIVISION OF BANKING

1714 Lincoln Avenue, Suite 2
Pierre, SD 57501
Phone: (605) 773-3421
Fax: (605) 773-3460

DATE: JULY 24, 2025

TO: ALL STATE-CHARTERED BANKS AND TRUST COMPANIES

FROM: BRADY SCHLECHTER, CHIEF INFORMATION SYSTEMS EXAMINER

RE: CYBER HYGIENE AWARENESS FACT SHEETS AND BOARD QUESTIONS: VULNERABILITY & PATCH MANAGEMENT/EVENT LOGGING & THREAT DETECTION

As part of our ongoing 2025 Cyber Hygiene Awareness campaign, we are pleased to provide the attached fact sheets for Vulnerability & Patch Management and Event Logging & Threat Detection. These documents are part of the third phase of our overall cyber hygiene campaign, which initiated in January. Additional issuances will be developed over the coming year to increase awareness and focus on critical cyber hygiene controls and practices already in place in your institution. These documents are not intended to introduce new guidance to the institution but are instead intended to spotlight and amplify best practices from existing regulatory guidance, CISA, the FFIEC IT Handbook booklets, and other authoritative sources that encourage comprehensive and consistent application of these cyber hygiene principles and practices, as well as increased oversight by senior management and the Board. Future releases will address additional cyber hygiene controls and practices, including incident response, cybersecurity awareness education, and data backup practices.

These fact sheets are intended for **CEOs** and **senior management staff** who can then share with **CISOs** and **IT security personnel**. These fact sheets provide a general overview of important cyber hygiene considerations to enable appropriate and consistent application of each practice. References are provided throughout each fact sheet to guide the reader to relevant source materials for each practice.

Board of Directors Resources

As part of this campaign, we recognize the value of providing resources to institution board members as well. Attached please find "Questions Board Members Should Ask" documents for Vulnerability & Patch Management and Event Logging & Threat Detection. These questions are intended to give the board structured questions to ask senior management to ensure that each practice has been appropriately implemented to protect the institution against cyber threats.

We strongly encourage you to share these documents with the appropriate staff within your institution.