National Federation of Municipal Analysts

White Paper on Best Practices in Cybersecurity Risk Disclosure for State & Local Governments in Municipal Offerings

EXECUTIVE SUMMARY

Every year, several hundred billion dollars of municipal bonds are issued and purchased by both institutional and retail investors. Cybersecurity is becoming an increasing concern of state and local governments, and cyberattacks against state governments, local governments, 501c3 organizations, and conduit borrowers **(together, the Issuers)** are becoming more commonplace. The costs to defend against cyberattacks and to remedy the damages caused by cyberattacks can be material, and present credit, fiscal and operational issues for Issuers. The municipal markets approach to cybersecurity event and risk disclosure is currently very ad hoc and incomplete. In addition, there is considerable variation in due diligence and disclosure practices of Issuers, underwriters,[1] and financial advisors as regards cybersecurity risks and events.

The National Federation of Municipal Analysts (NFMA) is concerned that all municipal bond investors have current, complete, and reliable information on cybersecurity risks and events so that market participants can make better informed investment decisions. Consequently, this NFMA White Paper (the White Paper) makes several recommendations to improve the primary offering and disclosure practices of Issuers and underwriters with regard to cybersecurity risks and events and includes recommendations for improved continuing cybersecurity event reporting and secondary market continuing disclosure. The NFMA acknowledges that law enforcement and insurance investigations may limit immediate or full disclosure of certain cybersecurity matters (including the problem of educating cybercriminals), but some minimal level of disclosure must be attempted when a government (or conduit borrower) suffers a serious cyberattack.

The NFMA hopes that recommendations in this White Paper will serve as a benchmark for improved cybersecurity risk and event disclosure practices by Issuers and underwriters. NFMA also seeks to promote increased dialogue with industry groups, regulators, and other interested parties on this important risk facing state and local governments. The NFMA believes that government issuers will ultimately benefit from these improved cybersecurity disclosure practices by broadening the investor base and interest for their bonds, and such increased interest/demand could result in "over-subscribed" transactions and tighter final bond pricing.

[1] As used in this White Paper, the term *underwriters* includes placement agents. The Securities Act of 1933 defines the term *underwriter* as "any person who has purchased from an issuer with a view to, or offers or sells for an issuer in connection with, the distribution of any security . . . ."

Please note that this White Paper does not constitute legal advice to any participant in the municipal bond market, including, among others, bond issuers, obligors, broker-dealers, and/or law firms. The White Paper represents NFMA's recommendation for disclosure practices based on our experience as municipal credit analysts and market participants, but recommendations included herein are not intended to constitute legal standards or any form of minimum disclosure requirements.

CONTENTS:

OVERVIEW: GOALS & LIMITS OF THIS WHITE PAPER

The NFMA is publishing this White Paper to address the growing importance of cybersecurity event and risk disclosure affecting state governments, local governments, 501c3 organizations, and conduit borrowers (together, the Issuers). This NFMA White Paper provides relevant background and context to cybersecurity disclosure issues in both primary market offerings and secondary market/continuing disclosure agreements. This White Paper also provides sample cybersecurity event disclosure covenants for indentures/loan agreements used in municipal offerings, as well as recommended due diligence questions for cybersecurity risk disclosures in primary market offerings. This White Paper briefly reviews the initiatives being undertaken by the SEC, public rating agencies, and industry groups to bring better focus on Issuer's cybersecurity risks, and Issuer's risk disclosure in primary municipal offering documents and secondary market continuing disclosure.

This White Paper is not intended to fully address all cybersecurity risks and issues confronting Issuers, nor the wide variety of systems, techniques, strategies and products that can reduce the risk of cyberattacks on Issuers. The NFMA recommends that all Issuers conduct a cybersecurity assessment to start the process of addressing cybersecurity risks as soon as possible. The NFMA encourages interested parties to submit comments at any time to lgood@nfma.org so that they can be considered in the development of future versions of this White Paper.

PART ONE: NFMA RECOMMENDATIONS FOR CYBERSECURITY RISK DISCLOSURE IN PRIMARY OFFERING DOCUMENTS (WITH SAMPLE CYBERSECURITY REPORTNG COVENANTS)

Currently, the NFMA, National Association of Bond Lawyers (NABL), Municipal Security Rulemaking Board (MSRB) and other municipal associations are wrestling with the need to address the extent to which Issuers must address cybersecurity issues in primary offering documents. The Security & Exchange Commission (SEC) has been taking an active role in cybersecurity risk assessments and disclosure for a while as regard to public companies. On February 26, 2018, the SEC issued the "Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures" (SEC Statement). The SEC Statement may provide Issuers with context and guidance on this topic. As SEC notes: "It is critical that all public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion". Clearly, the same disclosure responsibilities should apply to Issuers. Issuers facing a recent or ongoing cybersecurity attack may face a disclosure conflict: disclose the attack, payments made (if any) and the steps to prevent future cyberattacks versus educating/emboldening cybercriminals as to the results of their cyber-criminal activity and defensive measures taken by the Issuer. For purposes of this White Paper, we will call this the Cybersecurity Disclosure Conflict. Addressing new issue cybersecurity disclosure is challenging given the Cybersecurity Disclosure Conflicts, so the NFMA understands that its new issue disclosure recommendations will need to be tempered at times to minimize Cybersecurity Disclosure Conflicts.

Primary market offering statements are the best place for Issuers (including conduit borrowers like hospital borrowers) to address cybersecurity risks, cybersecurity events and cybersecurity mitigation strategies. When assessing the disclosure duties of Issuers, the primary rule is the Exchange Act Rule 10b-5 (Rule 10b-5), the well-known anti-fraud rule applicable to primary

securities offerings. While Rule 10b-5 has no express provisions regarding cybersecurity disclosure, the SEC's recent writings on cybersecurity clearly indicates SEC believes it is now a part of an Issuer's disclosure responsibilities.

Since cybersecurity risk and incident disclosure will vary between Issuers, the first step in the new issue cybersecurity disclosure process is the identification of existing cybersecurity incidents ("CI"). Individuals involved in primary offering due diligence (e.g., municipal advisor, underwriter, external or in-house counsel, etc.) may not always be aware of a CI incident during the crafting of primary market offering documents. Some CI may involve only temporary incapacity to access computer systems, external drives, and may not necessarily be part of a ransomware attack. CIs may also have occurred only with respect to a single business enterprise (sewer enterprise) or may have only affected a component unit. CI's may have been indirect, i.e., occurred with a large vendor/supplier that provides critical systems or supports to a Issuer (including utility providers). So, the first due diligence step in primary offering CI disclosure is to canvas key areas, teams, and component units of the Issuer, and expressly inquire about CI events. While staff education over CIs may not be very formalized at this point, deal participants doing due diligence should not overlook this education component and should seek to uncover CIs (including material threatened CIs) so as to better inform the due diligence professionals. One due diligence focus should be a phone call to the Issuer's insurance company to seek information on the Issuer's cybersecurity risk audit process (if any) and results.

CI threats may be more difficult to "ferret out" for various reasons including a government employee's natural inclination to downplay "threats" where they were made and no action resulted, the concern over disclosing cybersecurity protective strategies to would-be cyber criminals, and to prevent superiors from questioning the cybersecurity strength of systems designed and operated by the government employee. Actual and threatened cybersecurity attacks may be under active law enforcement investigation requiring some degree of confidentiality. Nevertheless, the primary offering due diligence process would require a cybersecurity "threat assessment" even if the results do not ultimately warrant any CI disclosure in the municipal offering documents. CIs threats should not be viewed solely as external third-party threats, but certainly can occur from internal disgruntled employees, fired employees, and temporary workers. So, CI due diligence needs to review both external and internal threats.

Where a CI (actual or threatened) is disclosed, Rule 10b-5 still requires a further assessment of materiality, which tends to be the province of the due diligence professionals. The frequency of CIs (actual and threatened) need to be assessed to assess materiality as well as the extent or scope of potential fiscal and government service disruptions. The materiality analysis is complex, and applying merely a fiscal/financial loss concept appears too narrow. CIs that disrupt delivery of information to suppliers, vendors, staff, and/or citizens may not have a direct or immediate quantifiable loss, but can harm the fiscal resiliency of the Issuer. In certain circumstances where there is an ongoing CI or CI investigation, there can be concerns over disclosure from an insurance or law enforcement perspective, so in these circumstances, certain details may need to be omitted by the Issuer from CI offering statement disclosure, but such restrictions should still be noted.

Cybersecurity risk disclosure can be approached both generically and with reference to material CIs if they have occurred. The cybersecurity risk disclosure section is not just about the risk and downside scenarios but is also be a good place to highlight an Issuer's cybersecurity risk

mitigation strategies (cybersecurity insurance; periodic third-party/insurance cyber risk audits; third-party cyber risk monitoring services; cybersecurity risk funds where the Issuer is self-insured). To the extent an Issuer has adopted formal cybersecurity risk protection protocols and systems, they should be described, and attention given as to why they are effective risk mitigation strategies. The existence of cybersecurity insurance policies should highlight coverage amounts/limits, deductibles, excluded events, and any other relevant policy terms. There are several levels and types of cybersecurity mitigation strategies especially as municipal enterprises like power, water, sewer, for example, will have different cybersecurity risks and risk mitigation strategies than general government services and operations. Generic cybersecurity risk disclosure will not be appropriate for a municipal offering pertaining to a municipal enterprise and vice versa, so some thought needs to be given by the underwriting teams so that the appropriate cyber risk disclosure is addressed and disclosed in the new offering document.

As many Issuers are just in the early phases of cybersecurity risk assessment and mitigation, robust cybersecurity risk mitigations may not be currently in place. In these circumstances, it will require honesty by the Issuer and its underwriting team to disclose this state of affairs. However, the cybersecurity risk disclosure section needs to provide a summary of the status of these efforts to date, and some idea of the timeframe for the cybersecurity risk assessment to be completed by the Issuer, and risk mitigation strategies assessed/implemented by the Issuer.

Conduit Issuers face a dilemma over the extent to which the underlying conduit borrower is able to undertake cybersecurity risk disclosure since many of these conduit borrowers are start-ups or newer companies that may not have had time or resources to address cybersecurity risks. In these situations, the underwriting/due diligence teams will need to undertake needed business line, industry, or sector research to identify "generic" cybersecurity risks faced by conduit businesses within this industry or sector. After making this review, the underwriting team should have the underlying conduit borrower identify relevant cybersecurity risks and address their resilience to CIs as best they can. Query if a special, third-party cybersecurity report needs to be undertaken and disclosed in the primary offering documents to overcome the lack of needed cybersecurity risk information in emerging industries (e.g., renewable fuel deals) and/or where the underwriting due diligence team lacks the needed cyber threat expertise.

PART TWO: NFMA RECOMMENDATIONS FOR POST-ISSUANCE CYBERSECURITY EVENT DISCLOSURE & CONTINUING DISCLOSURE AGREEMENTS

Issuers' continuing disclosure (secondary market disclosure) is a key area of concern for municipal investors, rating agencies, state/federal regulators and the public. Given the growing number of material CIs happening to Issuers, improved cybersecurity continuing disclosure is clearly warranted now – but how can it be effectuated systematically? Addressing post-issuance cybersecurity disclosure is challenging given the Cybersecurity Disclosure Conflicts noted above, so the NFMA understands that its secondary market disclosure recommendations will need to be tempered at times to minimize Cybersecurity Disclosure Conflicts.

There are at least four existing ways to address continuing disclosure of CI and other cybersecurity risks:

A. SEC Rule 15c2-12 event disclosures;
B. contractual covenants in bond documents (indenture, loan agreement, lease agreement, etc.) requiring cybersecurity risk mitigation and reporting of CIs;
C. more expansive continuing disclosure agreements to address CIs; and
D. Governmental Accounting Standard Board (GASB) financial statement disclosure in either the MD&A section or in the notes to the financial statements.

Each way has its advantages and disadvantages, so employing all four ways may be the most systematic and comprehensive way to address cybersecurity continuing disclosure. The NFMA has identified these advantages/disadvantages and offers some recommendations on best continuing disclosure practices for cybersecurity risks and CI.

The first option for municipal CI disclosure is SEC Rule 15c2-12 which requires certain material event continuing disclosure. The recently updated SEC Rule 15c2-12 has no express disclosures for CIs despite the fact certain CIs could be seen as material events affecting Issuers. The newly added 15c2-12(b)(5)(i)(C)(16) material event could cover a material loan covenant involving a cybersecurity event so long as it "reflects financial difficulties", but in many circumstances, an Issuer's CI may not immediately arise to the level of causing the Issuer "financial difficulties". The "financial difficulty" standard appears too restrictive and subjective to capture many cybersecurity risk disclosures of interest to the municipal market, and is also post-event disclosure only, i.e., it only captures large-scale CI damages that have occurred. So, on its own, the current SEC Rule 15c2-12 does not seem to provide a good vehicle for Issuer CI disclosure or cybersecurity risk mitigation disclosure by Issuers. While the SEC is concerned over cybersecurity risks to Issuers, that risk concern was not specifically addressed by SEC Rule 15c2-12, and given the time needed to adopt an updated SEC Rule 15c2-12 to address it, it is not likely to be addressed by SEC in the near term.

The second option for municipal CI disclosure is cybersecurity risks disclosure covenants in indentures, loan agreements, lease agreements and other Issuer debt documents (Municipal Bond Documents). While there is currently very little required cybersecurity risk disclosure in Municipal Bond Documents, the NFMA believes it is an ideal area for its development for several reasons. Adopting contractual provisions addressing cybersecurity risk mitigation and requiring CI disclosures in Municipal Bond Documents (Municipal Cybersecurity Covenants) has advantages, but seeking to implement those Municipal Cybersecurity Covenants will require the collective effort of municipal industry groups and associations to get Issuers, underwriters, bond counsel, underwriter's counsel to adopt these contractual provisions, and is one of the primary purposes of this White Paper. NABL has traditionally been the guardian of best practices in indenture contents for Issuers. NABL has both a model Trust Indenture for regular municipal issues and recently issued a model indenture for conduit municipal issues. Unfortunately, both NABL model indentures do not expressly address municipal cybersecurity issues or contain any Municipal Cybersecurity Covenants. Ideally, adding Municipal Cybersecurity Covenants to NABL's existing model indentures would be a significant step forward in getting appropriate Municipal Cybersecurity Covenants. Indentures are not the only type of Municipal Bond Document that can contain Municipal Cybersecurity Covenants, and loan agreements, lease agreements, and other municipal financing documents (Municipal Financing Documents) can contain Municipal Cybersecurity Covenants. These other documents would be the best vehicles for municipal conduit deals to address the cybersecurity risks of

501c3 borrowers, specialty municipal conduit borrowers and private borrowers. Municipal Cybersecurity Covenants contained in Municipal Financing Documents have at least three advantages:

A. They are binding and mandatory on the applicable borrower (compared to the lack of enforcement penalties for failure to make continuing disclosure agreement notices);
B. Non-compliance can create an event of default that does require 15c2-12(b)(5)(i)(C)(2) disclosure as a "non-payment" event of default; and
C. Municipal Cybersecurity Covenants can be crafted to address the particular cybersecurity risks of a particular borrower, industry and sector.

The NFMA can have a valuable role in crafting sector/industry appropriate Municipal Cybersecurity Covenants, and one goal of this White Paper is to identify what might be deemed "model" Municipal Cybersecurity Covenants in Appendix B below.

The third option for municipal CI disclosure is the continuing disclosure agreements (CDAs). Currently, the CDAs in the municipal market do not address municipal CI, but a simple addition to the CDA (very similar to the wording of Municipal Cybersecurity Covenants) could be used effectively to address municipal CI continuing disclosure. However, CDAs are currently not effectively enforceable by bondholders or trustees, and only permit a trustee or dissemination agent to file a "failure to file notice" on EMMA to alert the municipal market of an Issuer's failure to comply with a CDA – clearly an ineffective system. In addition, as municipal CI events are idiosyncratic, a municipal CI event would not be detectable by a trustee or dissemination agent unless it was so large and public that news reports would have alerted the trustee or dissemination agent to the need to disclose the municipal CI. Unlike the NABL model indenture, there does not appear to be an industry group that acts as the guardian of a "model" CDA although the GFOA has good CDA guidelines, and a few law firms have published a sample CDA forms. Certainly, the NFMA can facilitate developing a "model CDA", perhaps as part of a joint committee with various industry participants. So, until there is a "model" CDA, NFMA members will need to advocate for the inclusion of municipal DFI disclosures on an ad hoc/deal-to-deal basis.

Finally, the fourth option for municipal CI disclosure is the Issuers' use of the management discussion and analysis (MD&A) section of its financial statements (required by GASB) and the note section of the fiscal year end (FYE) financial statements. These two parts of GASB financial statements can be used to highlight material municipal CIs and provide appropriate context as to the financial effects of the municipal CI in the current fiscal year and subsequent fiscal years. While such a municipal CI note is not required supplemental information, an Issuer's failure to address a significant municipal CI in an Issuer's financial statements might cause a problem for the auditor and/or audit opinion. In any event, an Issuer's FYE financial statements are an ideal place to address municipal CIs in context, and to provide information to municipal investors, rating agencies, the public as regard to the cyber threats facing the Issuer and its mitigation strategies. Such financial statement disclosure may also have the positive effect of discouraging cybercriminals from cyberattacks for those Issuers touting their defenses to municipal CIs.

PART THREE: CYBERSECURITY EVENT DISCLOSURE – RECOGNIZING & ADDRESSING DISCLOSURE CONFLICTS

As noted earlier, Issuers facing a recent or ongoing cybersecurity attack may face a Cybersecurity Disclosure Conflict. Cybersecurity Disclosure Conflicts may not be open to an easy solution, and certainly cyberattack disclosure should be undertaken only after advice of law enforcement and trained counsel. For example, full cybersecurity disclosure may compromise an on-going law enforcement or insurance investigation. In addressing Cybersecurity Disclosure Conflicts, Issuers should consider the amount of detail needed to be disclosed against the compromise it may create in investigating/prosecuting a cyberattack. Municipal investors can appreciate that full candor may conflict with important law enforcement and insurance coverage concerns and can embolden efforts by unscrupulous third parties (taxpayers; accounts receivable payers, etc.) to take advantage of any disruption or compromise of an Issuers' invoicing and collection systems/records.

If there is a Cybersecurity Disclosure Conflict that is resolved by restricting the disclosure, that restriction decision should be noted in the disclosure itself to alert municipal investors that "the full story cannot yet be told". Full disclosure of the cyberattack should still be made when the disclosure conflicts are more readily in favor of full disclosure.

PART FOUR: RATING AGENCY VIEWS ON CYBERSECURITY RISKS FACING ISSUERS

All of the rating agencies are adding cybersecurity attack and resilience concerns in their risk analysis of state and local government operations; and are focusing on Issuer's proactive steps to address cybersecurity issues especially ransomware attacks. The rating agency approach to cybersecurity risk is not using any specific set of cybersecurity principles at this point. However, if an Issuer would suffer a material cybersecurity attack/disruption, the NFMA expects the rating agencies would initiate a rating review and, in certain circumstances, could find that a Negative Outlook is warranted if the cybersecurity attack was pervasive and a material comprise to key government operation and/or required a significant "ransomware" payment. In addition, once a material cybersecurity attack was disclosed, the NFMA expects rating agency scrutiny may not diminish until the Issuer has adopted more robust cybersecurity protection, and the rating agency has deemed them satisfactory.

PART FIVE: SEC VIEWS ON CYBERSECURITY DISCLOSURE

As noted earlier, the SEC Statement, though not specifically targeted to government Issuers, highlights disclosure guidance and best practice principles that are relevant to government Issuers. To quote the SEC Statement: "… it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack". Clearly, government issuers are under cyberattacks at this point and might take notice of the guidance given in the SEC Statement. Specifically, the SEC Statement discusses the use of the MD&A section of financial statements to provide an annual update on cybersecurity issues by public companies. In that regard, the SEC Statement notes: "In this context, the costs of ongoing cybersecurity efforts (including enhancements to existing

efforts), the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents, among other matters, could inform a company's analysis." The NFMA encourages Issuers to use their Management, Discussion & Analysis (MD&A) section of their annual GASB financial statements (or in the footnotes of their General Purpose Financial statements) to address their cybersecurity efforts in enough meaningful detail so as to inform municipal investors of the quality of management efforts to thwart cybersecurity events, but not "educating" cybercriminals unnecessarily.

PART SIX: GASB & AICPA CYBERSECURITY EVENT DISCLOSURE IN GOVERNMENT FINANCIAL STATEMENTS

Currently, GASB has no express guidance on financial statement disclosure of cybersecurity events although any large financial loss arising from a cybersecurity attack should be reflected in the Issuer's MD&A section of its financial statements or in the notes to the Issuer's financial statements (especially material ransomware payments). While the costs for a major cybersecurity risk mitigation system might generally not be large enough to warrant any special "line item" disclosure in its year-end financial statements, an Issuer certainly could devote a note in its financial statements to address the known cyber threats and fiscal risks associated with a historic cyberattack. In addition, the MD&A section of an Issuer's year-end financial statements affords an opportunity for it to highlight cybersecurity risk mitigation efforts and the costs therefor.

The American Institute of Certified Public Accountants (AICPA) also does not have any current governmental financial statement preparation or audit guidelines specifically pertaining to cybersecurity events. However, a government auditor may actually be a person who discovers evidence of a cyber incident during the audit process. Discovery of material cyber threat activity (especially if successful) may warrant a sentence in the audit opinion regarding the quality of the Issuer's financial control systems and cybersecurity systems. In addition, the auditor's letter to management may offer more candid assessment of an Issuer's vulnerability to cyberattacks. Government accounting firms can be used for special engagements to assess an Issuer's cybersecurity vulnerability and offer cybersecurity risk mitigation strategies/controls surrounding the Issuer's financial reporting system.

APPENDIX A: BACKGROUND - CYBERSECURITY THREATS TO STATE & LOCAL GOVERNMENTS; THE UNIQUE "PUBLIC NATURE" OF U.S. GOVERNMENTS & SYSTEMS

This appendix to the White Paper describes various types of cybersecurity threats and their effects on Issuers in the municipal financing space. U.S. state and local governments are uniquely "public institutions" with various state/local requirements over open records and open meetings laws. In addition, Issuers generally offer a higher degree of transparency to the public than does a private company. This unique public transparency creates more difficult cybersecurity challenges for Issuers than private companies. One goal of this White Paper is to assist Issuers in navigating the disclosures required by federal/state laws and municipal investor with this "public reality".

Issuers frequently find themselves in the crosshairs of cybercriminals. With 29.1% of local governments unaware of how often they are being targeted, and 47.1% percent attacked at least daily, Issuers are at risk of having their computer systems compromised (Norris, Joshi, Mateczun, & Finin, 2019). Cyberattacks are capable of crippling cities' day-to-day operations, including 911-services, transit fare collection, real estate transactions, utility bill processing, and tax collections. High profile attacks on Issuers like Atlanta and Baltimore showcase the need for potential investors to take a closer look at the susceptibility of Issuers' digital infrastructure and management teams' mitigation and contingency plans.

While Issuers have been reacting to the cybersecurity risk, more Issuer attention is needed to protect budgets and assets. A 2020 IBM Security survey (link?) of state and local employees found one in six respondents disclosed their state or local government department had been recently impacted by a ransomware attack, but only 38% received general ransomware prevention training. According to the 2019 State CIO survey (2019), only 31% of states had a formal marketing campaign to promote state awareness campaigns encouraging state cyber education efforts. However, states have been taking actions to address cybersecurity on an ad hoc basis. For example, the National Council of State Legislators reports that 31 states approved legislation or initiatives in 2019 on cybersecurity ranging from: training programs being required for government agencies; studies to assess block chain adaptions for cybersecurity; creation of new task forces to assess improved security practices; exempting cybersecurity operations from public information records laws; insurance industry regulation related to addressing cybersecurity loss prevention; required assessments and planning for utilities and critical infrastructure; and addressing cybersecurity threats to elections. In 2019, Illinois established a state department partnership to mitigate risks to elections and Indiana created a tool kit for local emergency managers. It should be noted that not all cyber threats are external; disgruntled existing employees can mount cyberattacks perhaps more effectively than an external cybercriminal.

1. Cyber Threats & Cyberattacks

Hackers use multiple ways to enter Issuers' cyberinfrastructure. Some of the most common methods include phishing emails, popular password attempts, and sending links that download malicious files when clicked. An infected computer can spread the virus to other susceptible and connected computers with or without immediately apparent symptoms. The virus can run in the

background while it, or the hacker, infects critical systems before seizing control of the infected files or systems.

Every day, more Issuers' systems are open to becoming targets for all types of hackers as the U.S. increases its reliance on connected automation, Internet-of-Things devices, and electronic databases for critical functions. Cybercriminals seek victims reliant on IT resources and target areas of cybersecurity weakness to steal information, monitor and disrupt operations, or extract financial resources (Moore, 2019). When an Issuer's agencies and departments vie for funding during the budget process, updating computer systems and information security often takes a backseat to media-friendly budget items (e.g., pensions, infrastructure projects, police & firefighter's salaries or jobs). Further, unprepared and underfunded IT security departments can make Issuer's government service deliveries (e.g., utility service, power-transmission, medical access, etc.) ever more susceptible to critical service disruptions.

The specific threats posed by cyberattacks on Issuers are as varied as the human imagination and depend largely on the purpose for which they are developed. Financially motivated attacks may steal banking information, reroute payments, or extort victims to release locked files. Countries may seek to quietly gather information or conduct cyber warfare activities. Additionally, some activists seek to disrupt operations that draw their ire. For example, in recent years, activists hacked the State of Michigan's website to bring attention to the Flint water crisis and North Carolina government websites to protest North Carolina's transgender bathroom use policies (Bergal, 2017). According to the University of Maryland-Baltimore County (2019), only 7.4% of local governments reported fewer total attacks year over year in 2018, illustrating that cybersecurity issues will not go away any time soon.

2. Denial of Service Attacks

In October 2016, the Mirai Botnet crippled much of the internet along the East Coast of the United States, however Mirai could have been directed at any target to flood servers with requests and deny operations (Fruhlinger, 2018). The Mirai Botnet is a distributed denial of service (DDoS) program that utilized common username and password combinations of hundreds of thousands of malware-infected Internet-of-Things devices. The Mirai Botnet code, other DDoS codes, and tutorials are available on the internet for other people to learn from and build upon (Fruhlinger, 2018). As more creative and talented individuals contribute to the internet's collective knowledge, new types of "denial of service" attacks against Issuers will likely emerge requiring organizations to remain up to date in the best methods of defending themselves.

3. Ransomware Attacks

Over the past several years, news sources have increasingly reported on cybercriminals' financially motivated ransomware attacks. Ransomware attacks lock down computer systems and servers by encrypting essential computer files and programs unless the victim pays the hacker a ransom (Blinder & Perlroth, 2018). While local governments are often a low-reward target for ransomware (only 17% of local governments paid the ransoms demanded, relative to 45% of all ransomware-affected entities), these numbers do not include the entities that may

have quietly paid a ransom without reporting the attack (Liska, 2019). Demanded ransom payments often pale in comparison to other direct and indirect costs to local governments seized by a cyberattack. The payments demanded ranged from $250-$400,000, and were less than 1.2% of revenues in all reported instances, excluding the City of Sarasota's $33M ransom, as of April 2019 (Liska, 2019). Local governments' costs to operate at the restricted capacity vary by the size of the entity and scope of operations, but attackers strategically demand low ransoms to incentivize payment (Blinder & Perlroth, 2018). However, costs to restore services are often more financially burdensome. For example, in the cities of Atlanta and Baltimore, the costs to restore services relative to the ransoms demanded were more than 293 times and 232 times respectively. As victims struggle to decide between restoring government services or paying criminals with taxpayer funds, the ransomware coders continue to innovate their products into a service-based industry.

The ransomware-as-a-service (RaaS) industry monetizes ransomware code packages with multiple pricing structures and features that may include up-front fees, percentage of ransoms paid, user friendly instructions to provide victims in how to make a payment, and advice to prevent the Issuer from being hacked again (Brenner, 2017). With the proliferation of RaaS on the dark web, anyone with a rudimentary ability for internet research could launch a ransomware attack against an Issuer for as low as $39 (Brenner, 2017). However, the ransomware services available for purchase can range from easily-tracked amateur products to invite-only partnership offers, such as GandCrab, which successfully ransomed an estimated $2 billion world-wide (Bennett, 2020). As Issuers are more likely than private companies to bring in Federal or state agencies for ransomware attacks and thereby generate "public" news coverage, attackers may leverage such notoriety as a marketing strategy to sell their RaaS product than on the direct financial gain from the ransom (Liska, 2019). With an initial fee, the RaaS model expands the developers' financial incentive of victims' payments to include generating demand for cybercriminal customers to purchase the coding package. Additionally, as many cybercriminals are located overseas, U.S. authorities' lack of jurisdiction in other countries makes arrest and prosecution of ransomware attacks against Issuers almost impossible (Grimes, 2016). The ransomware industry is likely to continue to innovate as the lack of legal jurisdiction, potential for large financial gains, and ease of access to cyberattack software enables extortionists to create income streams at low effort and low risk. Issuers will need to be constantly vigilant to try to stay "one-step ahead" of these cybercriminals and ransomware perpetrators.

4. Stealing Payment Information & Business Email Compromises

Another type of direct financial attack against Issuers is so-called business email compromises (BEC) which targets Issuers by infiltrating the email accounts of individuals who are responsible for wire transfer payments and fraudulently redirecting Issuer payments into accounts owned by the cybercriminal (Sherman, 2019). Cybercriminals have utilized BEC attacks to redirect millions of dollars in payments to contractors (Anderson, 2020). Smaller Issuers have sought out managed service providers (MSPs) to outsource their IT infrastructure and security needs to minimize BEC attacks. However, ProPublica (2019) reported that hackers are increasingly targeting and attacking these MSPs due to the potential to infiltrate multiple clients and thousands of computers with each MSP (Dudley, 2019).

Cyberattacks based on BECs are even a threat to municipal investors through disrupting normal Issuer pledged revenue collections (billing and collections) operations thereby compromising or delaying debt service payments, and even directly targeting Issuer debt service payments. For instance, an unnamed New Jersey municipality reportedly routed $40,000 of bond anticipation note debt service payments into a fraudulent account after a municipal officer fell victim to a BEC attack (Sherman, 2019). Additionally, Click2Gov, a self-service bill pay portal for utilities, community development and parking tickets, experienced two waves of breaches in dozens of cities across North America between 2017 and 2019, compromising the taxpayer payment information of over 320,000 payment cards (Alforov & Thomas, 2019). Issuers clearly face liability to their customers, taxpayers and service vendors if their payment information is stolen and used illegally. Such customer/taxpayer identity theft can severely erode confidence in an Issuer's ability to retain such valuable payment/identity information needed by the Issuer to sustain its cashflow and operations.

5. Government Infrastructure Threats & Compliance with Federal Cybersecurity Regulations

Issuers providing any type of utility services to its customers (electric, gas, water, steam, stormwater, sewer, etc.) and dedicated infrastructure Issuers like airports, port authorities, toll road managers, etc. all are subject to cyberattacks on their operations. Such cyberattacks could cause serious operations disruptions threatening the health and safety of thousands of individuals. In addition, Issuer systems that support inter-state commerce or other federally regulated activities (e.g., nuclear power plants) are subject to federal scrutiny of the Issuers' cybersecurity systems and response assets. For example, mandatory and enforceable federal regulatory standards are in place for electric utility systems' cyber and physical security. The North American Electric Reliability Corporation continues to address cybersecurity threats and risks by establishing industry regulations for all corporations and entities that work with bulk power system, as mandated by the Federal Energy Regulatory Commission. The Cybersecurity Act of 2015 requires sharing of cyber risk amongst utilities and have required grid level "cyberattack" planning and training.

6. Long-Term Collateral Damages to Issuers from Cyberattacks

A single successful Issuer cyberattack could potentially disrupt the functioning of essential government services needed for public health and safety, and generate a myriad of concerns with the public and investors. These cyberattacks can create long-term fiscal, reputational and legal issues for an Issuer. For example, a single robust Issuer cyberattack could lead to loss of records, systems and operations needed to properly and timely invoice and/or collect government taxes, fees, fines and other revenues. Such disrupted payment and collection activities could lead to Issuers facing near-term cashflow disruptions, the use of fund balances to cover cashflow shortfalls, and even the need to tap short-term lines of credit to support revenue collection and cashflow declines. In addition, an Issuer may need to free up needed funds to pay any demanded ransom to get a release of the cyberattack—and such unexpected ransomware payments can be large (over $1 million) and create additional cashflow concerns. If an Issuer decides not to pay a ransom (or does pay, but is not able to restore is record access/systems/storage), the Issuer will be facing significant costs to restore, retrieve, back-up its municipal records to a point where the

Issuer can restore its service capabilities. Lastly, the Issuer may still face the costs of improving its cybersecurity systems and retaining/training personnel to detect and fend off future cyberattacks. Multiple successful cyberattacks on an Issuer have the potential to degrade the financial profile of governments, their public bond ratings, and their ability to be trusted by the public, other Issuers, and their vendors; and can erode investors' confidence in the Issuer's ability to manage risks and operations. A classic case of the short-term and long-term collateral damage/effects of a cyberattack are chronicled in an S&P report on West Virginia Princeton Community Hospital illustrating the collateral damage that can come from a single Issuer cyberattack.

APPENDIX B: CYBERSECURITY RISK MITIGATION STRATEGIES – CYBER ASSESSMENTS, CYBER THREAT EDUCATION & RELIANCE ON EXTERNAL VENDOR CYBER THREAT MITIGATION PLANS/SYSTEMS

Cyberattacks continue to be a dynamic threat that require a dynamic response by municipal issuer/conduit borrowers. Municipal issuer/conduit borrowers may take several steps to prevent or mitigate the impacts of cyberattacks - buy insurance (if available), upgrade hardware, update software, hire specialized personnel, and train existing personnel to better identify, avoid, and report potential cyber threats. Municipal issuer/conduit borrowers should have a contingent operating plan in place to restore critical operations as quickly and efficiently as possible. In addition, municipal issuer/conduit borrowers need more robust data/system recovery plans to minimize the inevitable damages caused by a cyberattack including cloud-based data storage/retrieval. There are numerous firms, resources and products for municipal issuer/conduit borrowers to bolster their defenses and restoration capabilities presently available—and the best time to implement them is before a material cyberattack. Additionally, municipal issuer/conduit borrowers should reach out to federal and state agencies as well as industry associations (Government Finance Officers Association, "GFOA", National Association of State Treasurers, "NAST", etc.) for available resources to conduct cyber threat assessments, and discover tools, controls and programs to implement a more robust cyberattack defense and restoration plan. This White Paper is not intended to describe all the cyber-attack mitigation strategies, but here are some common strategies:

1. Upgrade Software, Hardware, & Source Quality Personnel

The threat of cyberattacks cannot ever be completely mitigated. However, municipal issuer/conduit borrowers can source quality IT personnel to proactively mitigate cyberattacks. Quality IT personnel can segment and monitor existing systems, upgrade outdated hardware, and maintain up-to-date software to greatly reduce the risk and impacts related to cyberattacks. These steps might be the most expensive pre-emptive actions; however, by targeting the systemic vulnerabilities, these steps have the highest chance of reducing the success rate of municipal issuer/conduit borrower cyberattacks. Additionally, municipal issuer/conduit borrowers should maintain clean offline backups. Clean office backups allow municipal issuer/conduit borrowers to quickly restore operations with minimal impact on government efficiency, financial costs, and revenue generation after a cyberattack. Smaller municipal issuer/conduit borrowers may seek an MSP to outsource their IT infrastructure but should still conduct due diligence to assess security vulnerabilities of the MSP to ensure their data is adequately protected.

2. Cyber Insurance

Municipal issuer/conduit borrowers may be able to procure some degree of insurance for cyberattack losses, but the coverage limits, excluded events, deductibles and insurance premiums may not make this a very ideal solution for all municipal issuer/conduit borrowers. Purchasing cyber threat insurance cannot be the sole defense to cyberattacks and in fact should only be part of a larger coordinated program to thwart cyberattacks. There is value in looking at cyber insurance since insurance companies have the staff, resources and expertise to make cyberattack assessments and recommend cyberattack mitigation strategies as part of an overall cyber insurance program. In purchasing cyber insurance, the insurance shifts most of the direct financial impacts to the insurance company (including liability defense costs), but having cyber insurance does not prevent the municipal issuer/conduit borrower from the operational and reputational impacts of a cyberattack. Municipal issuer/conduit borrowers should be aware that cyber insurance costs are likely to rise as the insurance market compensates for the frequency and fiscal severity of cyberattacks.

3. Increase Day-To-Day General Employee Cyber Awareness

Municipal issuer/conduit borrowers entrust their computer/data systems' integrity to their employees' ability to detect and appropriately respond to cyber threats (e.g., spoofing and suspicious emails). While trained IT personnel is a first line of defense, it requires "educated" employees to manage day-to-day the cyberattack vigilance. Such day-to-day cyber threat vigilance requires good educational programs for all employees offered at least once a year. While increasing employee competence in identifying, avoiding, and reporting potential cyberattacks should be a part of all cyberattack mitigation strategies, municipal issuer/conduit borrowers are now expected to go beyond that internal training and seek out more comprehensive, third-party cyberattack assessments, and implement their recommendations to the extent the municipal issuer/conduit borrower has the financial ability to do so. The cost of a municipal issuer/conduit borrower's cyberattack mitigation program can be material especially if critical government functions are exposed to cyberattacks.

The above recommendations are not exclusive nor exhaustive. For an informative article on resources available to municipal issuer/conduit borrowers and additional recommendations, refer to Lisa N. Thompson's (2019) article titled, *Cybersecurity Best Practices for Issuers* published in the New Hampshire Town and City magazine.

Robust cybersecurity mitigation strategies (such as external cloud storage/data backup systems) generally require third-party cybersecurity monitoring and attack detection, and third-party computer systems/data management. However, they also represent a new form of risk to municipal issuer/conduit borrowers in the form of vendor continuity and data access exposure. Third-party software/cloud/computer system vendors do go out of business, drop lines of business and experience their own data storage/retrieval problems. Consequently, an municipal issuer/conduit borrower's cybersecurity disclosure should contain a brief description of the extent the municipal issuer/conduit borrower relies on third-party cybersecurity vendors, the municipal issuer/conduit borrower's plan for replacing such vendors if needed, the costs of the third-party vendor systems, and the extent to which the third-party vendors provide insurance to the municipal issuer/conduit borrower in the event of a vendor system crash and loss or corruption of government data. The municipal issuer/conduit borrower may decide to be self-

insured for these third-party vendor risks or may choose to get independent insurance for potential vendor data/system crashes, data corruption/loss and vendor employee cyber theft. In any event, the use of third-party cybersecurity systems does pose potentially disclosable risks to municipal issuer/conduit borrowers, and municipal issuer/conduit borrower disclosure of these items may be warranted to highlight these third-party reliance risks.

APPENDIX C: RECOMMENDED CYBERSECURITY RISK DUE DILIGENCE QUESTIONS FOR STATE AND LOCAL GOVERNMENT PRIMARY OFFERINGS

To start the development of good cybersecurity risk disclosure due diligence for municipal issuer/conduit borrower s, this NFMA White Paper recommends the following questions/areas of inquiry:

1. Has the municipal issuer/conduit borrower had any material cybersecurity attacks in last three years?

2. If Yes, describe the circumstances including the following:

   a) the areas of governmental operations/private operations affected
   b) the length of the cybersecurity disruption
   c) the steps taken by the municipal issuer/conduit borrower to address the disruption;
   d) the fiscal cost to address the disruption(s) (if quantified)
   e) the third-party resources used by the municipal issuer/conduit borrower to address the cybersecurity event
   f) the expected time-frame to resolve the problems created by the cybersecurity event

3. Does the municipal issuer/conduit borrower have cybersecurity insurance coverage? If so, what are its maximum limits and deductibles by covered risks?

4. What affirmative/voluntary steps is the municipal issuer/conduit borrower taking to minimize cybersecurity events? Has the municipal issuer/conduit borrower retained third-party professionals to assess cybersecurity risks an\d provide an assessment report? If not, why not?

5. If the municipal issuer/conduit borrower does not have cybersecurity insurance, how will the municipal issuer/conduit borrower self-insure for such risks, and what levels of self-insurance are deemed prudent by the municipal issuer/conduit borrower?

6. What policies/procedures are in place to restore or maintain critical operations in the event of a cyberattack? What is the order in which services/functions will be restored?

7. To what extent does the municipal issuer/conduit borrower outsource its cybersecurity to third-party vendor? If outsourced, what protections are available if the external vendor goes out of business, the cybersecurity contract is terminated or the municipal issuer/conduit borrower cannot access the system/cloud when needed? Does the municipal issuer/conduit borrower have insurance protection for such events?

8. How segmented are critical cyber infrastructure systems to prevent cross contamination?

9. How have personnel performed on recent spam/phishing tests? Frequency of tests?

10. What is the oldest operating system within the network? How important is upgrading computer systems to address cybersecurity threats?

11. How often do the issuer's or borrower's systems back up a segregated copy of data items, e.g., monthly, etc.?

12. When was your last cybersecurity audit? What were the primary findings and recommendations? Were recommendations implemented?

13. Does the municipal issuer/conduit borrower rely on third-party cybersecurity vendors/services that pose risks of vendor service disruptions, data loss/corruption that is not adequately covered by insurance coverage?

APPENDIX D: MODEL CYBERSECURITY BOND DOCUMENT REPORTING COVENANTS & CDA CYBERSECURITY DISCLOSURE ITEMS

To start the development of some "model" Issuer cybersecurity covenants, this NFMA White Paper offers the following covenant language for inclusion in the appropriate Bond Documents, in addition, these same proposed covenants can be used to craft needed CDA disclosure for cybersecurity items.

Section ____. Disclosure of Cybersecurity Incidents & Cybersecurity Risk Assessments:

1. The municipal issuer/conduit borrower shall promptly report to the Trustee, in writing, any cybersecurity incidents (Incident Notice) and post such Incident Notice on EMMA as a voluntary notice. The Incident Notice shall contain the following information (in each case subject to any applicable disclosure restrictions under law or requested by law enforcement) as well as any additional information needed to avoid any misrepresentation of the Cybersecurity Incident:

    a) The date on which the Cybersecurity Incident appeared to have occurred and its duration;
    b) A description of any statements associated with the Cybersecurity Incident, and the Borrower's best estimates of the reason for the Cybersecurity Incident and its perpetrators (internal or external). If the Cybersecurity Incident was a ransomware incident, the amount of ransom requested;
    c) The information, systems, assets or data that were subject to the Cybersecurity Incident;
    d) The adverse effects, if any, on the municipal issuer/conduit borrower 's assets, data and systems from the Cybersecurity Incident including the current estimate of any remediation and recovery costs from the Cybersecurity Incident;

e) The expected length of time needed to fully assess the damage caused by the Cybersecurity Incident, and the expected length of time needed to remediate and restore the municipal issuer/conduit borrower 's assets, data and systems from the Cybersecurity Incident;
f) Whether the municipal issuer/conduit borrower has any form of insurance coverage for the damages caused by Cybersecurity Incident and the potential recovery amount;
g) The likelihood that the municipal issuer/conduit borrower will be subject a further Cybersecurity Incidents of this type; and
h) The steps being taken by the municipal issuer/conduit borrower to reduce or thwart future Cybersecurity Incidents, and the length of time needed to implement such steps.

As used in this Section___, "Cybersecurity Incident" means an unauthorized action or attempt to infiltrate, disrupt, steal, corrupt, control, transfer, or alter the functioning and integrity of a computer system, software, hardware, middleware, data transmission system, data storage or retrieval system, algorithms used in a computer system, controls for any robotic devices or machine learning devices, whether such systems or data are owned by the municipal issuer/conduit borrower or constitute third-party support of the operations of the municipal issuer/conduit borrower . Cybersecurity Incidents shall include attempts to post false or leading information regarding the municipal issuer/conduit borrower, the municipal issuer/conduit borrower activities and the Municipal issuer/conduit borrower 's full-time employees, board members or agents on social media or other internet-based platforms.

2. The Municipal issuer/conduit borrower shall maintain adequate vigilance and systems to thwart Cybersecurity Incidents at all times and shall retain internal or external professionals in detecting and thwarting Cybersecurity Incidents if there is a reasonable likelihood of a Cybersecurity Incident. The Municipal issuer/conduit borrower shall adopt a written policy regarding detecting and thwarting Cybersecurity Incidents which shall be reviewed and updated annually and shall comply with any applicable insurance carrier standards. Municipal issuer/conduit borrower shall have at least one permanent employee allocated to training to detect Cybersecurity Incidents and shall undertake to assess the cost and coverage for cybersecurity insurance annually as part of the municipal issuer/conduit borrower 's annual insurance coverage updates.

3. The municipal issuer/conduit borrower agrees that any Cybersecurity Incident will be treated as a "material event" for purposes of any continuing disclosure agreement which is binding on the municipal issuer/conduit borrower and subject to the same public posting requirements as any other material events.