SPRING 2021
www.bdo.com

BDO

Brixey & Meyer

THE NEWSLETTER OF THE BDO INSTITUTE FOR NONPROFIT EXCELLENCE℠

NONPROFIT STANDARD

IRS ISSUES FINAL REGULATIONS ON UBTI "SILOS"

By Marc Berger, CPA, JD, LLM

On Dec. 2, 2020 the U.S. Treasury and IRS published final regulations under Internal Revenue Code (IRC or Code) Section 512(a)(6), the provision requiring tax-exempt organizations with more than one unrelated trade or business to calculate unrelated business taxable income (UBTI) separately with respect to each trade or business. The provision, which was added to the Code by the 2017 tax law often referred to as the Tax Cuts and Jobs Act (TCJA), is known as the UBI "Silo" provision. The final regulations provide guidance on how an exempt organization determines if it has more than one unrelated trade or business and, if so, how the organization calculates UBTI under Section 512(a)(6).

The final regulations generally follow the approach taken in the proposed regulations (issued in April 2020), while making a few modifications based on comments received from tax-exempt organizations and practitioners.

IDENTIFYING SEPARATE UNRELATED TRADES OR BUSINESSES

Similar to the proposed regulations, most unrelated business activities must be classified using the first two digits of the North American Industry Classification System (NAICS) code that most accurately describes the trade or business. The IRS considered one commenter's view that the NAICS 2-digit codes be used as a safe harbor and that a facts and circumstances test be applied as the primary method of identifying separate unrelated trades or businesses. In rejecting that suggested change the IRS noted that adopting a facts and circumstances test would offer exempt organizations less certainty and likely result in inconsistency among exempt organizations conducting more than one unrelated trade or

CONTENTS

STAY CONNECTED to the **BDO Nonprofit & Education Practice** by following us on our

BLOG
nonprofitblog.bdo.com

on Twitter
@BDONonprofit

www.bdo.com/resource-centers/institute-for-nonprofit-excellence

CONTINUED FROM PAGE 1
UBTI "SILOS"

business because of differing approaches exempt organizations would take in applying such a test. It further stated that a facts and circumstances test would increase the administrative burden on the IRS which, upon examination, must perform the same fact-intensive analysis on each of the unrelated trades or businesses identified by the exempt organization.

In clarifying how an exempt organization should choose an NAICS 2-digit code, the IRS reiterated that the choice of the code must focus on the separate unrelated trade or business activity engaged in, and not the NAICS 2-digit code that describes the activities the conduct of which are substantially related to the exercise or performance of the organization's exempt purpose or function. For example, a college or university exempt under Section 501(c)(3) cannot use the NAICS 2-digit code for educational services to identify all of its separate unrelated trades or businesses.

One area that the final regulations differed from the proposed regulations concerns the ability to change an NAICS 2-digit code once it has been selected and reported on Form 990-T. The proposed regulations generally provided that, once an organization has identified a separate unrelated trade or business using a particular NAICS 2-digit code, the organization cannot change the NAICS 2-digit code describing that separate unrelated trade or business unless two requirements are met. First, the exempt organization must show that the NAICS 2-digit code chosen was due to an unintentional error. Second, the exempt organization must show that another NAICS 2-digit code more accurately describes the unrelated trade or business. In response to numerous comments on this issue, the final regulations remove the restriction requirements for changing NAICS 2-digit code(s). Instead, the final regulations require an exempt organization that changes the identification of a separate unrelated trade or business to report the change in the taxable year of the change in accordance with forms and instructions. To report the change, the final regulations require an organization to provide certain information with respect to each separate unrelated trade or business the identification of which changes: (1) the identification of the separate unrelated trade or business in the previous taxable year, (2) the identification of the separate unrelated trade or business in the current taxable year, and (3) the reason for the change. The IRS anticipates that the instructions to the Form 990-T will be revised to provide instructions regarding where and how changes in identification are reported.

ACTIVITIES DEEMED SEPARATE TRADES OR BUSINESSES

As provided under the proposed regulations, certain activities are treated as separate trades or businesses under the final regulations.

Investment Activities

The proposed regulations provided an exclusive list of an exempt organization's investment activities that may be treated as a separate unrelated trade or business for purposes of section 512(a)(6). Under the proposed regulations, for most exempt organizations, such investment activities are limited to: (i) qualifying partnership interests; (ii) qualifying S corporation interests; and (iii) debt-financed properties. Although commenters recommended modifications to the rules regarding the individual items included in this list, no commenters objected to the treatment of these items as investment activities. The final regulations adopt this list of investment activities without change.

Similar to the proposed regulations, the final regulations permit the aggregation of qualifying partnership interests (QPIs) into one separate unrelated trade or business in order to reduce the administrative burden of obtaining information from the partnership regarding its underlying trade or business activities where its percentage interest level indicates that the exempt organization does not significantly participate in the partnership. QPIs are generally defined as partnership interests that meet one of two tests: (1) **A de minimis test**, which the exempt organization satisfies if it holds directly or indirectly no more than 2% of the profits interest and no more than 2% of the capital interest of the partnership; or (2) **A participation test** (formerly known as the "control test" under the proposed regulations), which the exempt organization satisfies if it holds directly or indirectly no more than 20% of the capital interest and does not "significantly participate in" (formerly "control") the partnership.

As modified by the final regulations, an exempt organization significantly participates in a partnership if:

- The exempt organization, by itself, may require the partnership to perform, or prevent the partnership from performing (other than through a unanimous voting requirement or through minority consent rights), any act that significantly affects the operations of the partnership;
- Any of the exempt organization's officers, directors, trustees, or employees have rights to participate in the management of the partnership at any time;

CONTINUED FROM PAGE 2

UBTI "SILOS"

- Any of the organization's officers, directors, trustees, or employees have rights to conduct the partnership's business at any time; or
- The organization, by itself, has the power to appoint or remove any of the partnership's officers or employees or a majority of directors.

Similar to the proposed regulations, the final regulations require the interests of certain supporting organizations and controlled entities to be combined with those of the of the exempt organization in determining whether the organization's interest crosses the participation test's 20% threshold. One difference, however, is that the final regulations do not require an organization to combine the interests of a Type III supporting organization unless that supporting organization is the organization's parent.

In making the determination whether an exempt organization's interest in a partnership meets one of the two tests to be a QPI, the final regulations follow the rule in the proposed regulations that an exempt organization's percentage interest is determined by averaging the organization's percentage interest at the beginning of the partnership's tax year with its percentage interest at the end of that same partnership tax year. The final regulations, however, now provide a grace period when a change in an organization's percentage interest is due entirely to the actions of other partners. The grace period permits a partnership interest that fails to meet the requirements of either test because of an increase in the current year's percentage interest may be treated as meeting the requirements of the de minimis test or the participation test that it met in the prior year for the taxable year of the change if: (1) the partnership interest met the requirements of the de minimis test or the participation test in the organization's prior taxable year without application of the grace period; (2) the increase in percentage interest is due to the actions of one or more partners other than the exempt organization; and (3) in the case where a partnership interest met the participation test in the prior taxable year, the interest of the partner or partners that caused the increase in the current year was not one that was combined with the exempt organization's interest as described in the preceding paragraph in either the prior or current year.

With respect to qualifying S corporation interests (QSIs), the final regulations clarify that the exempt organization can rely on the Schedule K-1 (Form 1120-S) that it received from the S corporation if the form lists information sufficient to determine the organization's percentage of stock ownership for the year. For example, a Schedule K-1 that reports "zero" as the organization's percentage interest in the S corporation is not sufficient to determine the organization's percentage of stock ownership for the year. The IRS is considering whether revision of Schedule K-1 is needed to provide the information necessary to determine whether an S corporation interest is a QSI.

With respect to debt-financed income, several commenters suggested that this income should be reportable using an NAICS 2-digit code instead of as an investment activity. The final regulations rejected this suggestion and adopted the proposed regulations treatment as a separate investment activity.

Finally, the transition rule included in both IRS Notice 2018-67 and the proposed regulations, which permitted an organization to treat any partnership interest acquired prior to Aug. 21, 2018 as a single trade or business activity, will lapse as of the first day of the organization's taxable year following the issuance of final regulations. Despite receiving several comments asking the Treasury Department and the IRS to adopt the transition rule as a grandfather rule, it was not so adopted in the final regulations.

Payments from Controlled Entities

Similar to the proposed regulations, all "specified payments" (i.e., interest, rents, royalties and annuity payments per Code Sec. 512(b)(13)) received by a controlling tax-exempt organization from an entity it controls (i.e., more than 50 percent controlled by the organization) are treated as gross income from a separate unrelated trade or business. Moreover, if a controlling organization receives specified payments from two different controlled entities, the payments from each controlled entity would be treated as a separate unrelated trade or business.

Certain Amounts from Controlled Foreign Corporations (CFCs)

Similar to the proposed regulations, amounts included in UBTI under Section 512(b)(17) are treated as income derived from a single separate unrelated trade or business.

OTHER ITEMS OF NOTE

Allocation of Expenses – Pending the publication of further guidance in a separate notice of proposed rulemaking, the final regulations continue to provide that an exempt organization with more than one unrelated trade or business must allocate deductions between separate unrelated trades or businesses using the reasonable basis standard described in Treas. Reg. Section 1.512(a)-1(c).

Net Operating Losses (NOLs) – Under Section 512(a)(6), NOLs arising in a tax year beginning before Jan. 1, 2018 ("pre-2018 NOLs") may be taken against aggregate or total UBTI, while NOLs arising in a tax year beginning after Dec. 31, 2017

CONTINUED FROM PAGE 3

UBTI "SILOS"

("post-2017 NOLs") may only be taken against UBTI from the same trade or business from which the post-2017 NOL arose. The final regulations require an organization with both pre-2018 NOLs and post-2017 NOLs to first deduct its pre-2018 NOLs from its total UBTI before deducting any post-2017 NOLs from the UBTI of the separate trade or business that gave rise to the NOL. The final regulations further provide that if a trade or business is terminated, sold, exchanged or disposed of, any NOLs remaining after offsetting any gain on the sale or disposition are suspended. Suspended NOLs may only be used if the previous business is later resumed or if a new business using the same NAICS 2-digit code is commenced or acquired. For this purpose, a business is considered "terminated" if the appropriate identification of the business changes from one NAICS code to a different NAICS code.

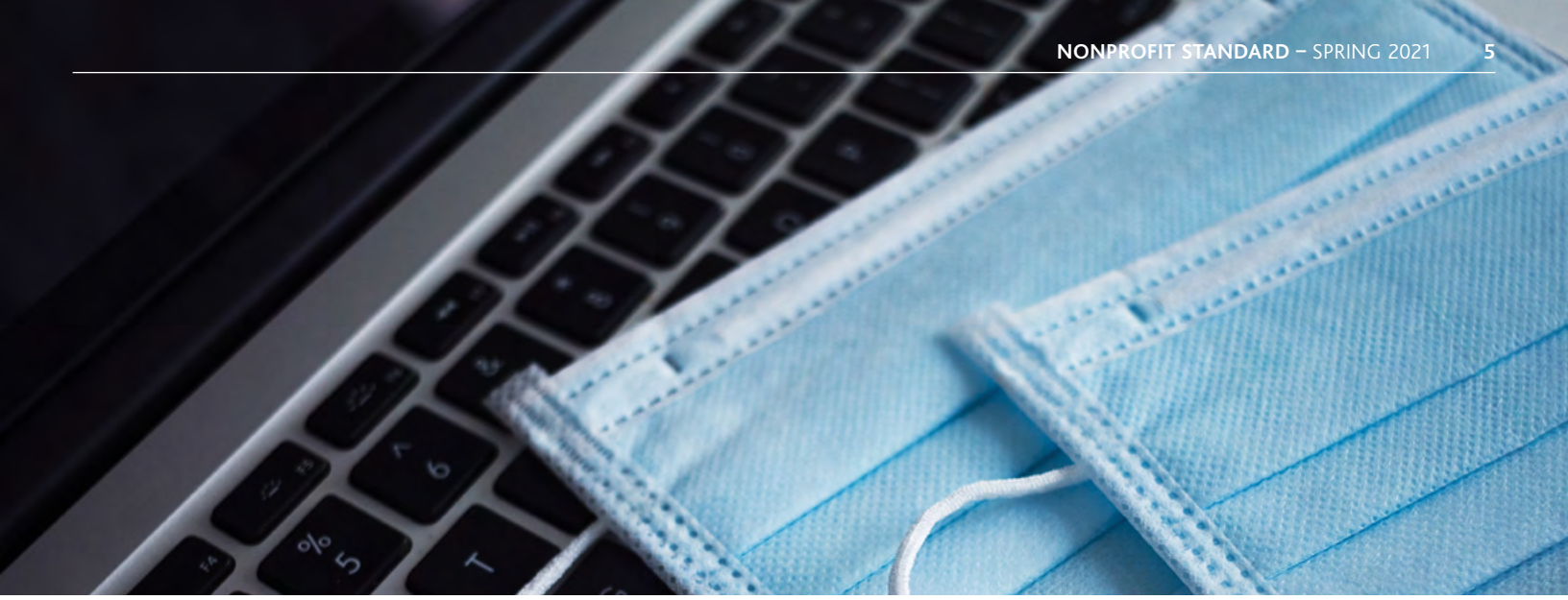
Charitable Contributions – Under Section 512(b)(10), tax-exempt corporations can take charitable contribution deductions under Section 170 up to 10% of UBTI (tax-exempt trusts look to Section 512(b)(11) for its percentage limitations). The final regulations provide that in applying these percentage limitations, exempt organizations would use total UBTI computed pursuant to Section 512(a)(6) and would not allocate the charitable contribution deduction among silos.

Public Support Tests – The final regulations address the fact that the calculation of public support on Form 990, Schedule A could be negatively impacted by the treatment of UBTI under the new silo rules. To address this issue, the final regulations allow exempt organizations to calculate public support tests using either UBTI as computed under Section 512(a)(6) or UBI calculated in the aggregate, whichever is least administratively burdensome or provides the highest ratio for the organization.

Subpart F and Global Intangible Low-Taxed Income – Similar to the proposed regulations, the final regulations clarify that inclusions of Subpart F income under Section 951(a)(1)(A) and global intangible low-taxed income (GILTI) under Section 951A(a) are treated in the same manner as dividends for purposes of Section 512(b)(1).

The final regulations are applicable to tax years beginning on or after Dec. 2, 2020 (date of publication in the Federal Register). For virtually all exempt organizations this means their 2021 tax years. Organizations should consult with their tax advisors to ensure the identification of any and all of their separate unrelated trades or businesses, especially those organizations with significant investment activities.

For more information, contact Marc Berger, National Director Nonprofit Tax Services, at mberger@bdo.com.



PROVIDER RELIEF FUNDS – REPORTING AND AUDIT REQUIREMENTS

By Carla DeMartini, CPA, Chad Krcil, FHFMA, CHFP, and Venson Wallin, CPA, CGMA, CFE, CHC, FHFMA, CHFP, HCISPP

When Congress passed the Coronavirus Aid, Relief and Economic Security (CARES) Act, it established the Provider Relief Fund (PRF) to support American families, workers and healthcare providers in the battle against COVID-19.

Through the CARES Act and supplemental funding from the Coronavirus Response and Relief Supplemental Appropriations (CRRSA) Act, the U.S. Department of Health and Human Services (HHS) is in the process of distributing $178 billion to hospitals and healthcare providers on the front lines of the coronavirus response and relief efforts. Qualified providers of healthcare, services and support may receive PRF payments for healthcare-related expenses or lost revenue due to COVID-19. While these distributions do not need to be repaid to the U.S. government, assuming providers comply with the terms and conditions established by HHS, these funds come with unique compliance, reporting and audit requirements that recipients must adhere to once they attest to the receipt of these funds.

REPORTING REQUIREMENTS

On Jan. 15, 2021, HHS released updated guidance on the PRF reporting requirements. Below, we outline what has changed since their last communication on Nov. 2, 2020. This amended guidance is in response to the CRRSA Act, which was passed in December 2020 and added $3 billion to the PRF (increasing the total funding from $175 billion to $178 billion) along with new language regarding reporting requirements.

Please note this is a summary of information and additional detail and guidance can be found in the reporting and auditing FAQ section of HHS.gov.

- On Jan. 15, 2021, HHS announced a delay in reporting of the PRF. HHS has not yet communicated further details on the deadline for this reporting. Recipients of PRF payments greater than $10,000 may register to report on their use of funds as of Dec. 31, 2020 starting Jan. 15, 2021. Healthcare providers should go into the portal, register and establish an account now so that when the portal is open for reporting, they are prepared to fulfil their reporting requirements.
- Recipients who have not used all of the funds by Dec. 31, 2020, have from January 1 – June 30, 2021 to use the remaining funds. Healthcare organizations will have to submit a second report before July 31, 2021 on how funds were utilized for that six-month period.
- The new guidelines further define the reporting entity and how to report if there is a parent company with subsidiaries for both General and Targeted Distributions:
  - Parent organizations with multiple Taxpayer Identification Numbers (TINs) that received General Distributions or TINS that received them from parent organizations can report the usage of these funds even if the parent was not the entity that completed the attestation.
  - While a Targeted Distribution may now be transferred from the receiving subsidiary to another subsidiary by the parent organization, the original subsidiary receiving the Targeted Distribution must report any of the Targeted Distribution it received that was transferred.

CONTINUED FROM PAGE 5

PROVIDER RELIEF FUNDS

- The new guidance does state that distribution of Transferred Targeted Distributions will likely fall under increased scrutiny through an audit by the Health Resources and Services Administration (HRSA).

- The calculation of lost revenue has been modified by HHS through this new guidance. Lost revenue is calculated for the full year and can be calculated using one of the following methods:
  - Difference between 2019 and 2020 actual patient care revenue. The revenue must be submitted by patient care mix and by quarter for the 2019 year.
  - Difference between 2020 budgeted and 2020 actual patient care revenue. The budget must have been established and approved prior to Mar. 26, 2020. This budget, as well as an attestation from the CEO or chief financial officer that it was submitted and approved prior to Mar. 26, 2020, will have to be submitted.
  - Reasonable method of estimating revenue. An explanation of the methodology, why it is reasonable and how the lost revenue was caused by coronavirus and not another source will need to be submitted.
- Recipients with unexpended PRF funds in full after the end of calendar year 2020, have an additional six months to utilize remaining funds for expenses or lost revenue attributable to coronavirus in an amount not to exceed the difference between:
  - 2019 quarter one to quarter two and 2021 quarter one to quarter two actual revenue,
  - 2020 quarter one to quarter two budgeted revenue and 2021 quarter one to quarter two actual revenue.

AUDIT AND COMPLIANCE REQUIREMENTS

Based on current information from HHS, provider relief funds are also subject to audit if more than $750,000 has been expended during an entity's fiscal year.

Over the next two years, many entities, which have received PRF exceeding the $750,000 threshold, may require an audit for the first time. For nonprofit, for-profit and government entities, this would result in a Single Audit under the Office of Management and Budget's (OMB) *Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards* (Uniform Guidance). A program-specific audit option may also be available under 2 Code of Federal Regulations (CFR) 200 Subpart F Section 200.501(c), if an auditee expends federal awards under only one federal program (excluding Research and Development). HHS has also noted that for-profit entities that received these funds have a third option, which would be a financial audit under **Generally Accepted Government Auditing Standards** (GAGAS) also referred to as the Yellow Book. There is still pending guidance from HHS around this third option in the areas of expenditures versus receipts, disclosures and timing of the report. However, what is fairly certain is that this type of audit would be conducted under Section AU-C 805, *Special Considerations- Audits of Single Financial Statements and Specific Elements, Accounts or items of a Financial Statement*, and will require the inclusion of a Statement of Costs and Lost Revenues in relation to any HHS federal awards.

Additionally, there may be some confusion and uncertainty among recipients who require a Single or program-specific audit for the first time. These auditees may be unfamiliar with audit expectations and preparations that need to take place in order to respond to federal compliance requirements. Determination of what should be reported on the schedule of expenditures of federal awards (the SEFA) may be challenging at first, especially since federal guidance surrounding the PRF has been continuously evolving.

There are some timing nuances and questions on what amounts (i.e., expenditures and lost revenues) should be reported for PRF (CFDA 93.498) on the SEFA by recipients for fiscal year-ends prior to Dec. 31, 2020. The "Other Information" section in the PRF section of the **OMB Compliance Supplement Addendum** (Addendum) issued on Dec. 22, 2020 addresses this by stating that "PRF expenditures and lost revenue will not be included on SEFAs until Dec. 30, 2020 year-ends and later." Rather, for fiscal years ended earlier than Dec. 30, 2020, recipients will report the 2020 93.498 expenditures and lost revenue in the 2021 audit. Keep in mind that this timing provision only affects the PRF program and is not applicable to other COVID-19 funding that healthcare entities may have received such as CFDA 93.461, *COVID-19 Testing for the Uninsured* or CFDA 93.697, *COVID-19 Testing for Rural Health Clinics*. For fiscal years ended Dec. 30, 2020 and later, the amounts reported on the SEFA (expenditures and lost revenue) should match the amounts submitted in the calendar year-end reporting required to be made directly to the HHS portal.

The deadline for the submission of the Single Audit reporting package to the Federal Audit Clearinghouse (FAC) is within the earlier of 30 calendar days after the single audit report's issuance, or nine months after year end. However, per OMB Memo M-21-20 issued Mar. 19, 2021 an extension has been provided that permits recipients and subrecipients that have not filed their single audit as of Mar. 19, 2021 that have fiscal year ends through June 30, 2021, to delay the completion and submission of the single audit reporting package to six months beyond the normal due date. There is no requirement for individual recipients and subrecipients

CONTINUED FROM PAGE 6

PROVIDER RELIEF FUNDS

to seek approval for the extension, but recipients and subrecipients should maintain documentation of the reason for the delayed filing.

NEXT STEPS FOR PRF RECIPIENTS

In the wake of this new guidance, PRF recipients should take the following steps:

- Register in the HHS portal and establish an account as soon as possible.
- Revisit lost revenue calculations to determine if current methodology is appropriate or if an updated methodology would be more appropriate under the new guidance.
- Understand the ability to transfer General and Targeted distributions and the impact on reporting of these funds.
- Develop reporting procedures for lost revenue and increased expense for reporting in the HHS portal.
- Confirm whether your organization is subject to the single audit. For preparation tips, visit BDO's Single Audit FAQ.
- Review audit and compliance requirements that pertain to your organization.
- For additional information about PRF compliance, audit and reporting requirements and answers to common operations, download BDO's PRF FAQ.

Article adapted from the Nonprofit Standard blog.

For more information, contact Carla DeMartini, assurance director, at cdemartini@bdo.com,

Chad Krcil, director, Industry Specialized Services, at ckrcil@bdo.com, or

Venson Wallin, managing director, Industry Specialized Services at vwallin@bdo.com.

SPOTLIGHT ON HIGHER EDUCATION

HIGHER EDUCATION EMERGENCY RELIEF FUND II

By Andrea Taylor

The Higher Education Emergency Relief Fund II (HEERF II) was authorized by the Coronavirus Response and Relief Supplemental Appropriations Act, 2021 (CRRSAA), which was signed into law on Dec. 27, 2020. In total, the CRRSAA authorizes $81.88 billion in support for education, $21.2 billion of which is now available to institutions of higher education to ensure learning continues for students during the COVID-19 pandemic. Allocations to institutions are based on a formula that includes the relative shares of federal Pell Grant recipients, the relative shares of non-Pell Grant recipients, and the relative shares of federal Pell and non-Pell Grant recipients exclusively enrolled in distance education prior to the coronavirus emergency. CRRSAA continues to support the important work of addressing students' unmet needs by providing a minimum amount of funding that each institution must devote towards financial aid grants to students. Institutions that were previously approved for Coronavirus Aid, Relief, and Economic Security Act (CARES Act) HEERF awards are not required to submit a new or revised application to receive additional funding under the CRRSAA.

HEERF II has some similarities—as well as important differences—from the CARES Act HEERF funding allocated to institutions in the Spring of 2020. HEERF II provides certain changes and flexibilities by expanding the allowable uses of funding as the COVID-19 pandemic continues to impact the enrollment, instruction and the overall financial health of many institutions. Some important changes include:

- **Expanded the allowable uses of grant funds** – In contrast to HEERF awards provided under the CARES Act, HEERF II's allowable uses include defraying expenses, including lost revenue and reimbursement of expenses already incurred.
- **Modified the share of funds that must be used for financial aid grants to students** – The CARES Act required that 50% of an institution's HEERF allocation be used to award financial aid grants directly to students. The CRRSAA requires that an institution receiving funding under HEERF II provide the "same amount" in financial aid grants to students from the new CRRSAA funds that it was required to provide under its original CARES Act HEERF allocation. Because this law appropriates more funding for supplemental and new awards to institutions, it is anticipated that a larger share of HEERF II allocations will be available for institutional support than under the CARES Act.
- **Added allocations for students enrolled in exclusively distance education courses** – Students enrolled in exclusively distance education courses are included in the CRRSAA allocation formula. Institutions will now receive allocations that factor in such students under the formula, and the formula also allows exclusively online institutions that were ineligible for funding under the CARES Act to apply for grant funds. Amounts apportioned for students enrolled in exclusively distance education courses may be used only for financial aid grants to students.

Institutions should regularly check the HEERF II CRRSAA website for the latest CRRSAA information and program guidance.

For more information, contact Andrea Taylor, assurance senior manager, at ataylor@bdo.com.

PRESENTATION OF COVID-19 RELATED FEDERAL PROGRAMS ON THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS

By Amy Guerra, CPA

New aid provided by federal agencies in response to the COVID-19 pandemic can impact the presentation of your organization's Schedule of Expenditures of Federal Awards (SEFA), Notes to the SEFA, and Federal Audit Clearinghouse Data Collection Form (DCF). As you prepare for your audit, it is important to understand the funding you received and identify the COVID-19 related funds separately on the SEFA provided to the auditors to support an effective audit.

Various federal programs provided new aid in response to the COVID-19 pandemic. Certain funds are subject to single audit, which requires recipients to prepare an SEFA. Federal agencies may have incorporated COVID-19 funding into an existing program and CFDA number or established a new COVID-19 program with a unique CFDA number. Federal agencies are required to specifically identify COVID-19 awards, regardless of whether the funding was incorporated into an existing program or a new program.

If an entity receives COVID-19 funds and makes subawards, the information furnished to the subrecipients should distinguish the subawards of incremental COVID-19 funds from non-COVID-19 subawards existing under the program.

All COVID-19 funding is required to be identified as such per Appendix VII of the OMB 2020 Compliance Supplement (Supplement). To maximize the transparency and accountability of COVID-19 related award expenditures, non-federal entities should separately identify COVID-19 expenditures on the SEFA by presenting this funding on a separate line by CFDA number with "COVID-19" as a prefix to the program name. The following

CONTINUED FROM PAGE 8

COVID-19 RELATED FEDERAL PROGRAMS

is an example of such presentation based on the OMB 2020 Compliance Supplement Appendix VII.

COVID-19 Temporary Assistance for Needy Families	93.558	$1,000.00
Temporary Assistance for Needy Families	93.558	$3,000.00
Total – Temporary Assistance for Needy Families		$4,000.00

In addition to separately identifying COVID-19 expenditures on the SEFA, there are new disclosures related to COVID-19 assistance that needs to be incorporated in the notes to the SEFA. Federal sources may have donated personal protective equipment (PPE) to an organization for the COVID-19 response. Nonfederal entities that received this donated PPE should provide the fair market value at the time of receipt as a stand-alone footnote accompanying their SEFA. As the donated PPE does not impact the single audit, the stand-alone footnote may be marked as "unaudited." PPE that is purchased using federal funds provided to the entity should be reported as federal expenditures.

The amount of donated PPE should not be counted for purposes of assessing whether your organization is over the $750,000 threshold of federal expenditures used to determine if a single audit is required. Donated PPE would also not count toward the Type A and Type B threshold for major program determination.

If a nonprofit organization is subject to single audit, it also requires a DCF submission to the Federal Audit Clearinghouse. At this time the instructions to the DCF have not been amended but entities should follow the OMB Compliance Supplement guidance to show the COVID-19 programs separately. The OMB Compliance Supplement recommends that the COVID funds should be entered on a separate row by CFDA number with "COVID-19" in the "Additional Award Identification" column. See example below:

As you prepare your internal SEFA be sure to follow this guidance.

	a	b	c	d	e	f	g	h
Row Number (auto-generated)	CFDA#		Additional Award Identification	Federal Program Name	Amount Expended	Cluster Name	Federal Program Total (auto-generated)	Cluster Total
	Federal Awarding Agency Prefix	CFDA Three-Digit Extension			($)		($)	($)
1	93	558		TEMPORARY ASSISTANCE FOR NEEDY FAMILIES	$3,000,000.00		$4,000,000.00	
2	93	558	COVID-19	COVID-19 – TEMPORARY ASSISTANCE FOR NEEDY FAMILIES	$1,000,000.00		$4,000,000.00	
				Total Federal Awards Expended =	$4,000,000.00			

For more information, contact Amy Guerra, assurance director, at aguerra@bdo.com.

CARES ACT EMPLOYEE RETENTION CREDITS FOR NONPROFIT EMPLOYERS

By Carolyn Smith Driscoll, Gabe Rubio, Brad Poris

Many nonprofit organizations were forced to shutter or temporarily close their operations under a governmental order as a result of the coronavirus pandemic, while others were forced to severely limit their offerings. One way to continue to pursue your organization's objectives is to ensure that you are still able to function, even if only in a limited capacity. The government has supported nonprofits and the continuation of their services with the passage of the Coronavirus Aid, Relief and Economic Security (CARES) Act in March 2020, which includes the Paycheck Protection Program (PPP) and the Employee Retention Credit (ERC). Under the CARES Act, organizations could take advantage of either the PPP or the ERC, but not both. In welcome news for nonprofit organizations, the Consolidated Appropriations Act, 2021 (Relief Act, signed by former President Trump on Dec. 27, 2020) **retroactively** eliminates this limitation and extends and enhances the ERC through the first two quarters of 2021. The ERC is one of the most beneficial provisions of the Relief Act relevant to nonprofit organizations. If you did not consider the ERC in 2020, or were not eligible to consider the ERC because you took a PPP loan, the retroactive ability to benefit from both PPP loans and the ERC is a powerful reason to consider the ERC for 2020. Looking ahead to 2021, the enhanced amount of the credit for wages paid during the first two quarters of 2021 provides another compelling reason to consider the ERC.

CAN NONPROFIT ORGANIZATIONS TAKE ADVANTAGE OF THE ERC?

Yes! Tax-exempt organizations are eligible for the ERC because they are deemed to be engaged in a trade or business regarding the entirety of their operations. Examples of nonprofit organizations that have already taken advantage of the credit are hospitals, schools, museums, performing arts centers and churches.

WHAT IS THE ERC?

The ERC is a refundable payroll tax credit for wages paid and health coverage provided by an employer whose operations were either fully or partially suspended due to a COVID-19-related governmental order or that experienced a significant reduction in gross receipts. The ERC can be claimed quarterly to help offset the cost of retaining employees. Employers may use ERCs to offset federal payroll tax deposits, including the employee FICA and income tax withholding components of the employer's federal payroll tax deposits. Unlike the PPP, which was on a first-come, first-served basis, the ERC can be claimed up to three years from the date in which your quarterly payroll return was filed.

CONTINUED FROM PAGE 10

CARES ACT EMPLOYEE RETENTION CREDITS

WHO IS ELIGIBLE FOR THE ERC?

To claim the ERC in any given calendar quarter, nonprofit organizations must meet one of the following criteria during that quarter:

- Operations were fully or partially suspended as a result of orders from a governmental authority limiting commerce, travel or group meetings due to COVID-19; or
- The organization experienced a significant decline in gross receipts during the calendar quarter compared to 2019. Specifically, for 2020, gross receipts for the 2020 quarter decline more than 50% when compared to the same 2019 quarter. Eligibility for the credit continues through the 2020 quarter in which gross receipts are greater than 80% of gross receipts in the same 2019 quarter.
- For 2021, the gross receipts eligibility threshold for employers is reduced from a 50% decline to a 20% decline in gross receipts for the same calendar quarter in 2019, and a safe harbor is provided allowing employers to use prior quarter gross receipts compared to the same quarter in 2019 to determine eligibility.
- Employers not in existence in 2019 may compare 2021 quarterly gross receipts to 2020 quarters to determine eligibility.

CAN YOU CLAIM THE ERC IF YOU RECEIVE A PPP LOAN?

Yes! As described above, one of the most favorable provisions in the Relief Act allows taxpayers to receive PPP loans **and** claim the ERC. This overlap was not permitted when the CARES Act was originally enacted, and organizations in need of cash infusions during 2020 more frequently turned to PPP loans as a source of funds rather than the ERC. Importantly, the Relief Act makes the ability to claim the ERC and receive PPP loans retroactive to March 12, 2020. As a result, organizations that received PPP loans in 2020 (and/or will receive new loans in 2021) can now explore potential ERC credits for 2020 and 2021.

WHICH WAGES QUALIFY FOR THE ERC?

The answer depends on an organization's employee count. Eligible organizations that are considered "Large Employers" can only claim the ERC for wages paid to employees for the time the employees are **not providing services**. This aligns with the purpose of the ERC, which is to encourage employers to retain and compensate employees during periods in which businesses are not fully operational.

Smaller eligible organizations may claim a credit for **all wages** paid to employees. The Relief Act increases the threshold used to determine Large Employer status for 2021 claims to an employee count of more than 500 (for 2020, it is more than 100). This favorable change broadens the number of eligible nonprofit organizations that can claim the ERC for all wages paid to employees, including wages paid to employees who are providing services. Importantly, qualified healthcare expenses count as wages.

BDO INSIGHT: If you furloughed your employees but continue to pay their health insurance, you can claim the ERC. Furloughed employees do not have to receive wages—health care expenses alone qualify as wages for purposes of the ERC.

HOW IS THE DETERMINATION OF LARGE EMPLOYER STATUS MADE?

Large Employer status is determined by counting the average number of full-time employees employed during 2019.

For this purpose, "full-time employee" means an employee who, with respect to any calendar month in 2019, worked an average of at least 30 hours per week or 130 hours in the month. This is the same definition used for purposes of the Affordable Care Act. Importantly, aggregation rules apply when determining the number of full-time employees. In general, all entities are considered a single employer if they are a controlled group of corporations, are under common control or are aggregated for benefit plan purposes.

Organizations that operated for the entire 2019 year compute the average number of full-time employees employed during 2019 by following the steps below:

Step 1: Count the number of full-time employees in each calendar month in 2019. Include only those employees who worked an average of at least 30 hours per week or 130 hours in the month.

Step 2: Add up each month's employee count from Step 1 and divide by 12.

BDO INSIGHT: Part-time employees who work, on average, less than 30 hours per week are not counted in the determination of Large Employer status. Omitting part-time employees from the computation should result in more nonprofit organizations having 500 or fewer full-time employees and, therefore, being able to claim the ERC for all wages paid to employees in the first two quarters of 2021 (assuming eligibility criteria are met).

CONTINUED FROM PAGE 11

CARES ACT EMPLOYEE RETENTION CREDITS

CAN THE SAME WAGES BE USED FOR THE COMPUTATION OF BOTH THE ERC AND THE AMOUNT OF PPP LOAN FORGIVENESS?

No. Simply put, there is no double dipping. Wages used to claim the ERC cannot also be counted as "payroll costs" for purposes of determining the amount of PPP loan forgiveness, and organizations that want to benefit from the ERC and have their PPP loans fully forgiven will need to have sufficient wages to cover both. To the extent an organization does not have sufficient wages, strategic planning will be needed to generate maximum benefits.

SUMMARY OF ERC CHANGES	PRIOR LAW: 3/13/20 – 12/31/20	NEW LAW: 3/13/20 – 12/31/20	NEW LAW: 1/1/21 – 6/3021
Interplay with PPP Loan	No ERC if a forgiven PPP loan was received	Taxpayers that receive a PPP loan can claim the ERC, but double dipping is not allowed	
Maximum Creditable Wages per Employee	$10,000 per year		$10,000 per quarter
Maximum Credit	50% of eligible wages, up to $5,000 per employee		70% of eligible wages, up to $28,000 per employee
Threshold to be Considered a "Large Employer" (based on average full-time employees in 2019 and considering aggregation rules)	More than 100		More than 500

BDO INSIGHT:

- Employers that previously reached the credit limit on some of their employees in 2020 can continue to claim the ERC for those employees in 2021 to the extent the employer remains eligible for the ERC.
- Qualification for employers in 2021 based on the reduction in gross receipts test may provide new opportunities for businesses in impacted industries.
- Eligible employers with 500 or fewer employees may now claim up to $7,000 in credits per quarter, paid to all employees, regardless of the extent of services performed. This rule previously was applicable to employers with 100 or fewer employees and a maximum of $5,000 in credit per employee per year. Aggregation rules apply to determine whether entities under common control are treated as a single employer.

For additional information, listen to BDO's archived Employee Retention Credit: Extended and Expanded Consolidated Appropriations Act of 2021 webinar.

Article reprinted from BDO Nonprofit Standard blog.


For more information, contact Carolyn Smith Driscoll, managing director and member of BDO's Business Incentives and Tax Credit practice, at csmithdriscoll@bdo.com,


Gabe Rubio, partner and member of BDO's Business Incentives and Tax Credit practice, at grubio@bdo.com, or


Brad Poris, managing director and member of BDO's Business Incentives and Tax Credit practice, at bporis@bdo.com.

NONPROFIT DATA BREACH VULNERABILITIES AND HOW TO AVOID THEM

By Mike Lee, CIPM, Alexandre Chanoine, J.D. and Derrick King

As more people are shifting to digital lifestyles and remote operations, data is being passed through the internet now more than ever. Proportionate to this, however, are the opportunities for potential compromise of the data, particularly via a data breach. Data breaches are the unauthorized access or disclosure of data for other than authorized and intended purposes. Nonprofit organizations, regardless of size, can be susceptible to a data breach as most accept and facilitate donations, which typically require the collection, processing, and maintenance of financial information. According to the Association of Certified Fraud Examiners 2020 Global Study, nonprofit organizations may be especially vulnerable compared to their for-profit counterparts as resources for privacy/security infrastructure are oftentimes harder to allocate. In recent years, cybercriminals have sought to harvest data for their own gain, targeting nonprofit donor and even employee data systems.

COMMON CAUSES OF DATA BREACHES

Data breaches can transpire and come in various forms. Per *The NonProfit Times*, about 75% of data breaches originate from outside the organization via malicious hackers and phishing activities, while approximately 25% stem from internal sources. The following are some of the most common causes of breaches:

- Lack of organizational privacy/security infrastructure, which incidentally is the part an organization can control. Privacy practices and controls (whether administrative or technical) may not appear as a high return on investment, but they can and will eventually be a good use of organizational resources. Do not let this be an afterthought.
- Human error or negligence – everyone has an "oops" moment, whether it's accidentally sending an email to an unintended recipient, attaching the wrong file or falling for a phishing attack. These are common honest mistakes absent malicious intent and can be remediated through mandatory privacy trainings, privacy awareness campaigns or administrative announcements reminding employees to secure the data they process.
- Ransomware and phishing attacks can and have been extremely damaging to organizations and individuals. Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid to the actor. Phishing is the fraudulent act of sending emails posing to be from a reputable company in order to trick individuals into providing their personal data, such as passwords or credit card information. When in doubt, if something doesn't appear to be for legitimate purposes or from a legitimate source, defer to your IT and privacy/security personnel.
- E-commerce hacks can occur if your organization uses an online store as a fundraising tool. Given the volume of payment information collected and stored, this opens up donors' personal data to compromise if not adequately secured.
- Despite the move to digital platforms and mediums, stolen hardware and/or physical files can still be compromised. It may be a laptop left in the backseat of a car that was just broken into or data that was physically mailed out without a tracking mechanism and can't be located. Users should always be cognizant of the data they process and maintain—especially outside of their normal work environment.

RECENT NONPROFIT DATA BREACHES

Nonprofit organizations have incurred significant breaches in recent years, both in terms of volume of records compromised, as well financial losses. The following are several examples—each by an external party—with varying results that may be surprising.

- In May 2019, a New York-based social services agency, suffered a breach of upwards of 1,000 of its clients' personal data when two of their employees' email accounts were hacked. Per the organization's official notice of the incident, the personal data breached may have included full names, addresses, Social Security numbers, financial account information, medical information, health insurance information and/or driver's license or other government identification numbers. Following initial detection and reporting of the breach, the agency reset the passwords for the hacked accounts.
- A Connecticut-based charity fell victim to a nearly $1 million cyberscam in May of 2017. Hackers were able to use the email account of a U.S. employee to create false invoices and other documents to trick the organization into sending nearly $1 million to a fraudulent entity in Japan. Unfortunately, by the time the breach was detected, the transfer had already cleared. However, the organization was able to recoup all but $112,000 via its insurance policy.

CONTINUED FROM PAGE 13

NONPROFIT DATA BREACH VULNERABILITIES

- A Charleston, S.C. cloud-based fundraising vendor for nonprofits and educational institutions, incurred a ransomware attack in early 2020 before it was detected in May of the same year. You know how they say, "Never pay the ransom?" The vendor paid the ransom. However, before receiving confirmation that the data had been destroyed, the attackers copied personal data from approximately 6 million clients—including donors, potential donors, patients and other stakeholders. Among the heavily impacted clients were Inova Health, Saint Luke's Foundation and MultiCare Foundation.

BEST PRACTICES TO PREVENT DATA BREACHES

Past data breaches suffered by nonprofit organizations provide us with lessons learned, which can then be leveraged into best practices. Consider the following to bolster your organization's privacy/security framework and minimize exposure to risks:

- Leverage external resources to identify and cover any privacy/security gaps. Perform a risk assessment to take inventory of what personal data is collected, used and managed to determine the risks associated with possessing the data. Purchasing cyber liability insurance can also help with providing comprehensive risk management insurance, and mitigate the financial impacts of a data breach. (See Mark Millard's article on page 15 for more information.)
- Fortify your donation platform's security. Work with IT, as well as any vendors to comply with applicable privacy/security regulations and standards, such as Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR). These are particularly relevant given the high utilization of credit card information.
- Regularly review and actively manage users' access permissions. Monitor and update role-based access for users who have access to data throughout business operations to ensure they only use what they need proportionate to their respective roles. This will also help mitigate the disgruntled former employee breach scenario.
- Implement data minimization controls, only collecting and processing what information is needed for authorized and legitimate business purposes. Similarly, implement and adhere to a data retention policy, only retaining what is necessary to accomplish the objectives and properly disposing of data when it is no longer needed.
- Ensure older and sunsetting technologies have been wiped of personal data prior to getting rid of them. Storing data in multiple locations and mediums helps mitigate hardware failure, but they still need to be accounted for prior to retirement.
- Report breaches, as soon as they are detected. While the point is to mitigate the risks if a breach occurs, the reality is that they are almost unavoidable. It is important to have dedicated incident/breach response policies and procedures, including tabletop activities to prepare for the inevitable breach. (A tabletop activity is a security incident preparedness activity, taking participants through the process of dealing with a simulated incident scenario and providing hands-on training highlighting flaws in incident response planning.)

CONCLUSION

Data breaches — the causes, impacts and consequences — can be devastating to an organization. As such, it is imperative to be prepared for what is unforeseen but nonetheless predictable. While this may seem daunting, particularly for smaller nonprofits, it should be emphasized that some of the most basic data privacy/security best practices and controls are easy to implement at little to no cost. Overall, the biggest step to be taken in protecting your organization and stakeholders is to make privacy/security a priority. Even without in-house resources, nonprofits can benefit from leveraging external ones to help augment policies and procedures. Preparing for this upfront will save a lot of trouble if a breach occurs.

For more information, contact Mike Lee, manager and member of BDO Digital's Governance and Risk Compliance group, at mrlee@bdo.com,

Alexandre Chanoine, senior manager and member of BDO Digital's Governance and Risk Compliance group, at achanoine@bdo.com, or

Derrick King, director and member of BDO Digital's Governance and Risk Compliance group, at dking@bdo.com.

ASSESSING RISK TO MAXIMIZE CYBER INSURANCE COVERAGE

By Mark Millard

It's 8 a.m. on Monday. You open the doors to the office, preoccupied with tasks for the week: grant applications that need review, donor phone calls to make, staff disagreements to manage, current program execution and strategy for the future. As you settle into your desk and turn on your computer, the startup screen displays a simple message: "Pay 100 Bitcoin to 123 account number in the next 12 hours or lose all of your data." Panic sets in, your mind races, all thoughts from two minutes ago have disappeared. What do you do next?

These days, this type of scenario is all too common. Some make headlines, but most don't and are dealt with quietly and quickly. The challenge with many nonprofits is they reside in a place of reaction when it comes to IT infrastructure, security and crisis management. Many nonprofits walk the tightrope of pressure to reduce administrative expenditures and improve programmatic spending. Often, donors look at operating percentages when choosing where they will make their gifts. This challenge creates difficulties in determining how much to spend on IT infrastructure and cybersecurity.

The exposure to cyber intrusion for a nonprofit is often not adequately understood and, as such, marginalized by thinking that because we do work for the "greater good," the entity won't be a target. Unfortunately, cybercrime focuses on the ease and reward of opportunity, thus making many nonprofits a perfect target. (See further discussion in the article on page 13.)

Before COVID, it was typical to find remote access driven by individual employees trying to find solutions to the work challenges and not organizationally driven by strategy. COVID and the exodus to a remote work environment have only exacerbated the issue. Many organizations have strung together technology solutions to meet the need for remote work. This rush to operationalize has been fraught with missteps and increased the risk for intrusion.

So what do you do with finite administrative dollars to spend? Do you spend the dollars on IT security and testing, training employees on proper cyber hygiene (e.g., “Don't click on that link"), crisis management and business continuity planning, or insurance? The answer is all of the above, while strategically prioritizing where you can't have everything on the shelf. Depending on your organization's IT security maturity, the quickest and most reliable risk mitigation you can take will be insurance. When adequately structured, it will be your most crucial risk mitigation effort.

Cyber insurance has been one of the fastest-growing and evolving products in the insurance market during the past decade. News of the mega-breaches that readily come to everyone's mind has driven this growth with many organizations recognizing the tremendous exposure to liability and business interruption resulting from a cyber intrusion. And what have we learned about cyber intrusions through the countless breaches we've read about over the years? They have many sources, are ever-evolving, impact organizations in different and unique ways and are challenging to stop, making a case for spending dollars on a cyber insurance policy that much more significant.

The problem we find with many organizations is their insurance approach and, more specifically, cyber insurance approach. Insurance is often a check the box mindset. Buy it once a year, pay a premium, receive an insurance policy and promptly place it in the drawer. This approach is always problematic, but less so for certain insurance types than others such as auto or workers' compensation insurance policies. Cyber insurance is the exact opposite of these aforementioned policies where there are standard forms and definitions and decades of claims experience providing a guide to what is and is not insured. Cyber insurance is the new kid on the block that everyone is still figuring out.

The cyber insurance marketplace is a highly fractured space that lacks a standard definition set and coverage provisions. There are over 100 insurance companies that underwrite the product with common coverages but little standardization.

For cyber insurance, most start with a basic coverage form. However, that form's value will depend on how well you understand your unique risk and negotiate the insurance policy's appropriate coverage. We've encountered many clients who purchased cyber insurance, put it in the drawer, checked the box and moved on with their lives. Then the claim showed up. Surprise, coverage denied. The conversation from there is typical: "Denied?!? I bought insurance for this." Yes, but you didn't buy the right insurance. You didn't understand your unique type and amount of risk, leading to the coverage gap. So what steps can you take to avoid this dreadful scenario and not spend precious funds doing so? Start by looking at the risk.

Broadly speaking, we bucket cyber risk into two categories; first-party and third-party losses. Or, in other words, damage to your organization's property and ability to conduct business (first party), and injuries to others due to your negligence (third-party).

CONTINUED FROM PAGE 15

CYBER INSURANCE COVERAGE

When determining the type of cyber insurance needed, we begin with risk management 101, identify the risk.

Risk can originate from an insider, whether intentionally or not, criminal hackers, hacktivists or third-party compromise. To understand your threat areas, start with a simple whiteboarding session with the key stakeholders in your organization—CEO, chief financial officer, Operations lead, IT, HR and others, and play through a few what-if scenarios to determine what would happen and the resulting operational and financial impact. Areas to focus on can include:

- Computer system damage and loss
- Data loss
- Business shutdown
- Fines and penalties
- Liability associated with data loss
- Reputational damage
- Theft of funds
- Extortion

It is essential to understand where these risks can stem from as insurance policies will have exclusions that limit coverage due to cause. For instance, an insurance policy might require that you provide all IT vendors' names that offer your organization services. The simple error of omitting one vendor can void coverage should the loss result from their services. Next, you will want to assign value to your risk areas to determine exposure to one or multiple impacts. Consider:

- The cost to replace your computer systems if required due to system bricking (damaged beyond repair, making the device unusable) for the first-party loss.
- Would you need to spend money to recreate data?
- Would you be subject to a business interruption where revenue generation would be reduced or ceased?
- Would you incur extra expenses to have temporary fixes or accelerate your recovery?
- How many personally identifiable information (PII) or protected health information (PHI) records do you maintain and what is the potential liability for losing these records?

As more and more entities are moving data to cloud storage, do not believe that this relieves you of liability exposure. In these instances, assessing risk transfer and protection through your contractual agreements will be important in addition to the protections you might take with insurance. Once you've built an understanding of individual risks and their value, you are ready to consider the type and amount of insurance to purchase.

Here is the good news. Cyber insurance options are plentiful, with broad coverage and reasonable prices compared to its early years. Obtaining a base cyber insurance policy for $1 million in limits can often be done for minimal cost. When purchasing cyber insurance, it will be critical to have a partner who understands the insurance coverage—further making this point. A recent advertisement from an insurer for NFP cyber insurance provided a listing of the policy coverages: Privacy Liability for release of PII or other corporate confidential data, network security liability, media liability and breach response costs. At first glance, this might look great. The policy will cover the third-party liability aspects. Also, it has coverage for breach response costs, which we will explore in a moment. But what is missing? There is limited first-party coverage and no coverage for system damage resulting from the breach. Given the check-the-box insurance approach discussed earlier, these insurance policies' deficiencies often go unnoticed until a claim arises.

So what should you look out for in a well-structured cyber insurance policy?

- **Privacy liability** – coverage for damages associated with the release of personal information
- **Network security liability** – coverage for failure to prevent an attack against your network
- **Media liability** – coverage for liability associated with content you create and distribute
- **Breach response costs** – coverage for direct costs associated with a breach (This can include credit monitoring, forensic and remediation services, and public relations costs.)
- **Property damage directly resulting from the breach** – coverage for replacement and repair of systems damaged from the breach
- **Income loss, extra expense and dependent business income** – coverage that protects against lost revenue due to a service disruption or network outage
- **Data recovery** – coverage for costs associated with recreating data lost or stolen
- **Extortion** – coverage for payment for a demand placed by the cybercriminal
- **System failure** – coverage for unintentional outage resulting from an error
- **Regulatory fines and penalties** – coverage for payment of fines assessed by a governing body associated with a breach

CONTINUED FROM PAGE 16

CYBER INSURANCE COVERAGE

In addition to these coverages, cyber insurance policies have evolved to provide liquidity relief and a service tool with crisis management, breach response and even some systems diagnostic services. Many cyber insurance policies offer a specific panel of specialists on call and available for the insured's use in a breach. For the nonprofit community, these additional services can be worth as much as the insurance policy's liquidity relief.

So as you look to spend your finite administrative dollars, a key part of your cyber risk mitigation strategy should focus on the purchase of a cyber insurance policy. When properly structured, it is the one protection you can count on when all other security measures put in place fail.

For more information, contact Mark Millard, managing director, BDO's Insurance Risk and Recovery Group, at mmillard@bdo.com.

REVISIONS TO THE UNIFORM GUIDANCE AFFECTING RECIPIENTS

By Tammy Ricciardella, CPA

On Aug. 13, 2020, the Office of Management and Budget (OMB) issued Final Guidance on amendments to the OMB Guidance for Grants and Agreements (Uniform Guidance). This reflects the first revisions to this guidance since they were originally issued in 2013. The impact from these revisions range from minor and unique circumstances to large-scale changes that affect all recipients. Thus, if you receive federal funding, it is important that you review the OMB revisions in their entirety to ensure you are familiar with these changes and implement necessary changes to your systems and provide appropriate training to your grants management and accounting personnel.

The revisions are generally effective for new awards issued on or after Nov. 12, 2020.

Following is a high level summary of certain of the noteworthy administrative type changes:

- 2 CFR 200.414(f) *De Minimis Rate* – this section permits entities with negotiated indirect cost rate agreements (NICRA) that have expired to use the 10% de minimis rate to calculate indirect costs.
- 2 CFR 200.414(h) *Publication of NICRAs* – this is a new section that requires certain information related to NICRAs to be collected and displayed on a public website. The information is limited to the indirect negotiated rate, distribution base and the rate type.
- 2 CFR 200.322 *Domestic Preferences* – this section encourages recipients to "maximize use of goods, products and materials produced in the United States."
- 2 CFR 200.320 *Methods of Procurement* – this section was amended to reflect the revised thresholds for micro-purchases at $10,000 and the simplified acquisition threshold at $250,000. This also permits recipients to request higher micro-purchase thresholds up to $50,000 from the agencies.
- 2 CFR 200.244 *Closeout* – OMB revised the time period for recipients to submit closeout reports and liquidate all financial obligations from 90 days to 120 days.

There were also certain clarifications of existing provisions that were made to provide clarity related to a pass-through entity's responsibilities. These revisions clarified that:

- Pass-through entities are responsible for addressing only a subrecipient's audit findings specifically related to its award.
- OMB directs pass-through entities to use a subrecipient's NICRA but, if none exists, the parties are to either negotiate a rate, use the de minimis rate, or subrecipient may use the cost allocation method to account for indirect costs.

As part of the update the provisions of the National Defense Authorization Act for FY 2019 was incorporated which prohibits the obligation or expenditures of federal funds and awards for the use of "covered telecommunications equipment or services." (See 2 CFR 200.216) This prohibition is effective Aug. 13, 2020.

For more information, contact Tammy Ricciardella, assurance director, at tricciardella@bdo.com.

OTHER ITEMS **TO NOTE**

SINGLE AUDIT SUBMISSION EXTENSION

The Office of Management and Budget (OMB) issued Memo M-20-21 (Memo) that instructs federal awarding agencies to allow recipients and subrecipients that have not yet filed their single audits with the Federal Audit Clearinghouse (FAC) as of Mar. 19, 2021 (the date of the Memo) with fiscal year ends through June 30, 2021, an extension to delay the completion and submission of their single audit reporting package for up to six months beyond the normal due date.

No action is needed by federal awarding agencies to enact this extension. Recipients and subrecipients do not need to obtain approval to utilize this extension. However, as with past extensions, recipients and subrecipients need to maintain documentation of the reason for the delayed filing.

Recipients and subrecipients who take advantage of this extension would still qualify as a "low-risk auditee" for their next year's audit.

It is important to note that this new 6-month extension is longer than the 3-month extension included in the OMB Compliance Supplement Addendum (Addendum). In addition, this extension applies to all single audits. The prior extension noted in the Addendum was only available to those who received COVID-19 funds.

OMB COMPLIANCE SUPPLEMENT ADDENDUM

OMB issued the long awaited Addendum to the Compliance Supplement on Dec. 22, 2020. The Addendum includes information on certain COVID-19 stimulus funds including the Provider Relief Fund, Coronavirus Relief Fund and the Education Stabilization Fund.

FASB APPROVES GOODWILL ALTERNATIVE FOR NONPROFITS

On Mar. 30, 2021 the Financial Accounting Standards Board (FASB) issued Accounting Standards Update (ASU) 2021-03, *Intangibles – Goodwill and Other (Topic 350) Accounting Alternatives for Evaluating Triggering Events*. This ASU makes a change to the accounting rules for nonprofits and private businesses that will help reduce the costs and complexity for accounting for goodwill.

Goodwill is often recorded when one entity purchases another entity for more than the value of the existing physical assets. Under the current accounting rules, entities must monitor and evaluate whether what is known as a triggering event may have occurred that could result in the value of the goodwill recorded being impaired.

Issues around identifying triggering events has become more apparent during the pandemic because of ongoing economic uncertainty.

For the majority of nonprofits and private companies this analysis is likely only performed annually at the date that the financial statements are prepared. The current accounting guidance that requires the assessment of a potential impairment as of the interim date creates difficulties for these entities.

This ASU will permit all nonprofits and private companies to utilize the option to perform the identification and evaluation of a triggering event for goodwill impairment as required by Accounting Standards Codification (ASC) 350-20 to be completed at either the end of a quarterly or annual period in line with their standard reporting periods. An entity that elects this alternative would not be required to monitor the goodwill impairment triggering event in interim periods but would instead evaluate the facts and circumstances as of year-end to determine whether it is more likely than not that goodwill is impaired.

The ASU is effective on a prospective basis for annual reporting periods beginning after Dec. 15, 2019. Early adoption is permitted for financial statements that have not yet been issued or made available for issuance.

This ASU is separate from a larger goodwill project that the FASB is working on, in which it is considering a requirement that entities write down a set portion of goodwill each year, instead of testing for potential impairment annually.

FASB REMOVAL OF CONSOLIDATION OF A NOT-FOR-PROFIT ENTITY BY A FOR-PROFIT SPONSOR FROM TECHNICAL AGENDA

The FASB (the Board) decided to remove the project related to consolidation of a not-for-profit entity by a for-profit sponsor from its technical agenda. The Board's research determined that this situation is not sufficiently pervasive to amend generally accepted accounting principles. The project was initially added to the agenda because based on initial research it was noted that there was diversity in practice and that for-profit sponsors predominantly do not consolidate sponsored not-for-profits in their financial statements.

UPDATES TO IRS MANDATORY E-FILING REQUIREMENTS FOR 2021

The IRS provided an update to mandatory e-filing requirements for 2021 in its Exempt Organizations (EO) Update. The updates noted are as follows:

- Tax year 2020 Forms 990-T and 4720 are being revised and will be available for e-filing in 2021.
- Transitional relief is available for Form 990-EZ for tax years ending before July 31, 2021.
- Forms 990 and 990-PF or tax years ending on and after July 31, 2020 must be filed electronically.